



Technologische Souveränität:

Vorschlag einer Methodik und
Handlungsempfehlungen

Inhaltsverzeichnis

Zusammenfassung	3
1. Warum bezieht der VDE Stellung?	4
2. Was ist mit „technologischer Souveränität“ gemeint?	5
3. Aspekte „technologischer Souveränität“	7
3.1. Dimension „Branchen“	7
3.2. Dimension „Technologiefelder“	7
3.3. Bewertung der Relevanz von Technologiefeldern	9
3.4. Dimension „Anforderungen an Souveränität“	11
4. Ausprägungen technologischer Souveränität	14
4.1. Grade souveränen Handelns	15
4.2. Beispielhafte Anwendung der Systematik	16
4.2.1. Beispiel 5G (Schlüsseltechnologie)	16
4.2.2. Beispiel KI / Data Science (Technologiefeld)	21
5. Position der ITG	26
5.1. Anforderungen zur Erreichung technologischer Souveränität	26
5.2. Maßnahmen zur Entwicklung technologischer Souveränität	26
5.3. Technologische Souveränität im breiteren (politischen) Kontext.	28
6. Schlussfolgerungen	29
Literaturverzeichnis	30
Anhang	31

Herausgeber: ITG

Editor: Dr.Klaus Illgner

Redaktionsteam: Prof. Roland Gabriel, Prof. Wolfgang Halang, Prof. Albert Heuberger, Dr. Klaus Illgner, Prof. Dorothea Kolossa, Prof. Sebastian Möller, Prof. Hans Schotten, Sigurd Schuster

VDE Verband der Elektrotechnik
Elektronik Informationstechnik e.V.
Stresemannallee 15
60596 Frankfurt am Main

Zusammenfassung

Technologische Souveränität ist die Fähigkeit eines Staates oder einer Gesellschaft, politische und gesellschaftliche Prioritäten umsetzen zu können, ohne dabei durch unzureichende oder fehlende Kontrolle über Technologien behindert zu werden. Sie ist von Autarkie einerseits und von Fremdbestimmung andererseits abzugrenzen. Klima- und Umweltschutz, Digitalisierung im Sinne der sozialen Marktwirtschaft und Datenschutz sind Ziele, deren Umsetzung von der Verfügbarkeit geeigneter Technologien abhängig sind. Die Bundeskanzlerin führt diesbezüglich am 11. September 2019 im Deutschen Bundestag als Beispiele für Technologien, in denen wir nur im europäischen Kontext wieder den Anschluss an die Weltspitze erreichen können, u. a. Mikroelektronik und Batteriezellenfertigung an.

Ziel dieses Positionspapieres ist, das Konzept der technologischen Souveränität tiefer zu diskutieren, zu analysieren, welche Voraussetzungen für Erhalt oder (Wieder-)Erlangung technologischer Souveränität zu schaffen sind, und insbesondere für das zentrale Technologiefeld der Informations- und Kommunikationstechnik (IKT) konkrete Empfehlungen zu formulieren.

Technologiefelder sind nicht mit Branchen oder Anwendungen gleichzusetzen, da diese in sehr verschiedenen Anwendungen zum Einsatz kommen können. Dieses Papier betrachtet Technologiefelder als eine für die Beurteilung der technologischen Souveränität relevante Dimension. Zur Identifikation und Bewertung von Technologiefeldern werden Kriterien vorgeschlagen, die neben wirtschaftlichen auch gesellschaftliche und politische Aspekte umfassen.

Ein wesentlicher Beitrag des Papiers liegt in der Bewertung technologischer Souveränität entlang einer generalisierten Wertschöpfungskette, da sich die Anforderungen an die technologische Souveränität erheblich mit der innerhalb der Wertschöpfungskette wahrgenommenen Funktionen unterscheiden. Das Papier konkretisiert, was „technologischer Souveränität“ bedeutet, indem es entsprechende Anforderungen für die verschiedenen Stufen entlang der Wertschöpfungskette beschreibt. Es stellt sich heraus, dass die konkrete Ausgestaltung der Souveränitätsanforderungen vom Technologiefeld abhängt, es zugleich aber auch übergreifende Gemeinsamkeiten gibt. Zur Quantifizierbarkeit werden unterschiedliche Souveränitätsgrade vorgeschlagen.

Die Methodik, Anforderungen an die technologische Souveränität entlang der Wertschöpfungskette zu erfassen, wird anhand des Technologiefeldes KI und der Schlüsseltechnologie 5G konkret vorgestellt. In der IKT brauchen wir eine ausgeprägte Befähigung zu souveränem Handeln, indem wir selbst über das technische Detailwissen verfügen, international relevante Forschung betreiben sowie eigene Infrastrukturen konzipieren, aufbauen und nutzen können. Da wir in der IKT die Komponenten überwiegend von internationalen Herstellern beziehen, müssen wir in der Lage sein, deren Vertrauenswürdigkeit selbst zu validieren und die Infrastrukturen umfassend selbst zu betreiben und zu warten. Wir brauchen Souveränität aber keine Autarkie, die es bei der Entwicklung von Technologien der ITK heute nicht mehr geben kann.

Aus Sicht der ITG haben Förderung der Ausbildung und Stärkung der Forschung eine sehr starke Hebelwirkung in der Gewährleistung technologischer Souveränität in aktuellen und zukünftig relevanten Technologiefeldern sowohl für die Wirtschaft (Entwicklung, Produktion, Nutzung) als auch für die Gesellschaft.

Die ITG will mit diesem Positionspapier einen branchenübergreifenden Prozess mit definierten Kriterien anstoßen, mit dem die relevanten Technologiefelder und die aktuell dahinterstehenden Schlüsseltechnologien identifiziert werden. Nur in interdisziplinärer Zusammenarbeit kann auf nationaler Ebene ein einheitliches Bild ermittelt werden, wo besondere Anstrengungen zum Erhalt bzw. zur (Wieder-)Erlangung technologischer Souveränität erforderlich sind und welche konkreten Anforderungen an die technologische Souveränität erwartet werden.

Im Sinne des von der Bundeskanzlerin beschriebenen europäischen Kontextes sind die Anforderungen an die technologische Souveränität auch aus europäischer Perspektive zu bewerten. Vor dem Hintergrund der aktuellen weltpolitischen Lage braucht Europa technologische Souveränität, welcher Grad in welchem Technologiefeld zu erreichen ist, ist zu ermitteln. Wo für eine einzelne Volkswirtschaft ein gewünschter Souveränitätsgrad unrealisierbar ist, so kann dies im europäischen Kontext durchaus möglich sein.

1. Warum bezieht der VDE Stellung?

Wir befinden uns inmitten einer gravierenden, substanziellen Umwälzung aller Lebensbereiche. Im Zuge der Digitalisierung durchdringen die Informations- und Kommunikationstechniken (IKT) alle Lebensbereiche und verändern deren Funktionalitäten, die wirtschaftlichen Konstellationen und letztlich die gesellschaftlichen Strukturen. Wir können uns auf das, was wir kennen, nicht mehr verlassen, da es so keinen Bestand haben wird.

Ausgelöst durch Cyberattacken, Spionage im Netz und die Veröffentlichung vertraulicher Informationen findet vorwiegend unter den Begriffen „digitale Souveränität“ und „technologische Souveränität“ eine Debatte statt, wie Vertrauen in IKT-Infrastrukturen erhalten oder hergestellt werden und wie wir unsere Handlungsfähigkeit erhalten bzw. wiederherstellen können.

Beispiel 2: Investitionszyklen versus technische Entwicklungsgeschwindigkeit

Die öffentliche Hand (inkl. des Militärs), aber auch Industriebranchen investieren in Infrastruktur und betreiben diese über sehr lange Zeiträume (zum Teil > 20 Jahre). Gerade Prozessanlagen laufen Jahrzehnte. Wie kann gewährleistet werden, dass auch nach Jahrzehnten noch Ersatzteile und Know-how für Betrieb und Wartung einer Infrastruktur (Hardware und Software) vorhanden sind? Zulieferer sind Stand heute vorwiegend außereuropäische Unternehmen, womit die Möglichkeiten zur Einflussnahme auf Produktlaufzeiten eher gering sind.

Darüber hinaus gibt es verschiedene Grade technologischer Souveränität. Wie „souverän“ möchte wer sein? Die Spannweite reicht vom Setzen auf die Kräfte des freien Marktes über das Erlassen (und Einfordern) von Regularien bis dahin, alles selbst herstellen und betreiben zu können (nationale Autarkie).

Das Positionspapier wendet sich primär an das Fachpublikum und die Politik. Sein Ziel ist, die volkswirtschaftliche und gesellschaftliche Bedeutung „technologischer Souveränität“ aufzuzeigen. Als Schlüsseltechnologie in allen Technologiefeldern bildet die IKT hierbei den roten Faden. Letztlich geht es darum, die Zukunftsfähigkeit unserer Volkswirtschaft und damit unsere gesellschaftliche Basis zu gewährleisten. Es wird eine strukturierte systematische Analyse angeregt, die insbesondere systemische Aspekte ausleuchtet und bewertet. Die Politik ist aufgefordert, alle Beteiligten zusammenzubringen, um ein gemeinsames Verständnis dessen auszuarbeiten, wer welchen Grad an Souveränität als sinnvoll erachtet und

Beispiel 1: Manipulation kritischer Infrastrukturen

Hackern ist es gelungen, sich in Stromversorgungsnetze einzuloggen und diese zu infiltrieren (Wet16), (NCA18). Krankenhäuser mussten ihren Betrieb wegen Ransomware einstellen. Persönliche Daten von Personen des öffentlichen Lebens (Journalisten, Politikern) wurden im Netz veröffentlicht. Dies sind nur ein paar Schlagzeilen, die verdeutlichen, dass Infrastrukturen alles andere als sicher sind und essentielle Infrastrukturen angegriffen werden können.

Die Diskussion offenbart, dass Sicherheit nur eine Facette ist. Fragen wie nach dem Zugang zu Technologien, Zugang zu Komponenten oder der Fähigkeit, selbst Infrastrukturkomponenten herstellen zu können, spannen einen weit größeren Bogen, der sich auch in der parallelen Diskussion wiederfindet, inwieweit Unternehmen von ausländischen Investoren kontrolliert / übernommen werden dürfen. Die so verstandene „technologische Souveränität“ adressiert ganz grundsätzliche wirtschaftspolitische Fragen.

Dieses Papier möchte einen Beitrag leisten, indem es die verschiedenen Definitionen von „digitaler Souveränität“ und „technologischer Souveränität“ in einer Art Landkarte zusammensetzt, aus der deren Spannweite abgeleitet werden kann. Es zeigt sich, dass „digitale Souveränität“ und die darin enthaltenen Sicherheitsaspekte in einen größeren Rahmen eingebettet sind.

Beispiel 3 – 5G in der Industrie

5G ist als Kommunikationstechnik in der Industrie z. B. für die Automatisierung von großem Interesse. Damit gehen hohe Anforderungen an die Zuverlässigkeit und die Sicherheit einher. Eine Anlage darf nicht von außen manipulierbar sein (z. B. eine Produktionsanlage für chemische Stoffe) und Daten (selbst Steuerdaten) dürfen aus Wettbewerbsgründen nicht an Dritte gelangen. Für die Industrie ist daher die vollständige Kontrolle der Infrastruktur unabdingbar. Wie lässt sich aber gewährleisten, dass die Infrastruktur sicher, vertrauenswürdig und zuverlässig ist?

welcher Grad an Souveränität in welchen Technologiefeldern aus wirtschaftlichen und politischen Gesichtspunkten erreicht werden muss. Gerade in gesellschaftlich relevanten Bereichen wie der Mobilität wird es politisch definierter Orientierungspunkte bedürfen. Auch sind die Sichtweisen der Beteiligten entlang einer generalisierten Wertschöpfungskette angefangen bei Bildung und Wissensmanagement über Forschung, Produktion, Betrieb bis hin zur Nutzung und deren gesellschaftlichen Auswirkungen unterschiedlich. Daraus können dann konkrete Maßnahmen abgeleitet werden. Wichtig ist, dass es nicht genügt, „technologische Souveränität“ und / oder „digitale Souveränität“ auf IKT-Sicherheit zu beschränken. Technologische Souveränität betrifft IKT, Energietechnik, Energieversorgung, Biotechnik / Bionik, Industrie und viele andere Bereiche. Letztlich sollte es für jedes Technologiefeld eine Position geben.

Beispiel 4 – Banken (Keu18)

Kapitalmärkte spielen eine zentrale Rolle für das Funktionieren einer Volkswirtschaft. Die Kontrolle über den Geldfluss haben bislang die Banken. Mit den digitalen Plattformen verändern sich die Geldströme und die Beteiligten, die die Geldströme kontrollieren / steuern. Die dominanten Player sind außer-europäische, privatwirtschaftliche Technologieunternehmen. Damit sind nationale Unternehmen (u. a. auch Banken) auf deren Wohlwollen angewiesen (vgl. Zugang zur NFC-Schnittstelle von Apple für die Banken). Welchen Einfluss auf Regelungen haben wir noch? Wieviel Kontrolle brauchen wir?

2. Was ist mit „technologischer Souveränität“ gemeint?

Mit dem Begriff „Souveränität“ bezeichnet man gemeinhin die Unabhängigkeit eines Staates gegenüber dem Einfluss eines anderen Staates, aber auch das Recht, frei nach eigenem Ermessen handeln zu können, sowie das selbstsichere Auftreten einer Person. Ursprünglich aus dem Französischen kommend umschreibt der Begriff auch die höchste Gewalt in einem Staat (der König als Souverän).

Wesentliche Merkmale der „Souveränität“ sind also eigenständiges und unabhängiges Handeln, das gerade auch die Befähigung zu eigenständigem Handeln einschließt. Souveränität umfasst nicht nur, nach eigenem Ermessen zu entscheiden, sondern auch letztlich die letzte (höchste / abschließende) Entscheidungsinstanz zu sein. Souveränität grenzt sich einerseits von Autarkie und andererseits von Fremdbestimmung ab.

Vor dem Hintergrund von Cyberangriffen gerade auch auf kritische Infrastrukturen, dem Ausspähen von Bürgern durch massenhaftes Abgreifen und Auswerten von Daten durch Geheimdienste und den Datensammlungen großer internationaler Konzerne wird über „digitale“ / IKT-Souveränität diskutiert. Viele Interessengruppen aus Wirtschaft, Gesellschaft und Politik haben sich hierzu bereits geäußert und Maßnahmen eingefordert (Bit15)(Mai15). So definiert auch der ZVEI (ZVEI15) „Digitale Souveränität“ als die Fähigkeit, Vertrauenswürdigkeit, Integrität sowie Verfügbarkeit von Datenübertragung, -speicherung und -verarbeitung durchgängig kontrollieren zu können.

Hierbei werden allerdings verschiedene Begriffe zum Teil synonym bzw. für teilweise identische Aspekte benutzt.

Den Begriff „digitale Souveränität“ definiert Wikipedia wie folgt: „Abgeleitet vom Begriff der Souveränität versteht man unter Digitaler Souveränität selbstbestimmtes Handeln unter vollständiger, eigener Kontrolle im Hinblick auf die Nutzung digitaler Medien“, was an anderer Stelle als „mediale Souveränität“ bezeichnet wird (Wik20).

Der Begriff „technologische Souveränität“ taucht in Deutschland erstmals 2011 im Zuge der Gründung des vom damaligen Innenminister Thomas de Maizière und vom damaligen CEO der Deutschen Telekom René Obermann initiierten Arbeitskreises SIKT „Sicherheit in kritischen IKT-Anwendungen und IKT-Architekturen“ auf, der eine Strategie zur „nachhaltigen Sicherung der IKT-kritischen Anwendung“ entwickeln sollte (Bau15). Technologische Souveränität wurde anhand von fünf verschiedenen Anwendungsbereichen geprüft: Geheimschutz und hoheitliche IKT, Identity Management, Intelligentes Fahrzeug, Smart Grid sowie Überwachung und Steuerung großtechnischer Anlagen (Bau15). Der Begriff „technologische Souveränität“ wird also überwiegend fokussiert auf Sicherheitsaspekte verwendet.

Das derzeit diskutierte mögliche Verbot von Huawei als 5G-Netzausrüster und die öffentliche Diskussion in Europa und den USA verdeutlichen, wie bedeutsam Vertrauen in die Systemhersteller kritischer Infrastrukturen ist. Es geht also nicht nur um Regularien, sondern auch um die Produktion der Komponenten der Kommunikationsinfrastruktur und den dahinterliegenden, bis ins „Eingemachte“ gehenden Einblick in die zugehörigen Netzelemente. Der Übergang von „digitaler Souveränität“ zur umfassenderen „technologischen Souve-

ränität“ ist also fließend. In die Debatte um Huawei fließen wirtschaftspolitische Aspekte ein, wenn von „Wettbewerbsfähigkeit vertrauenswürdiger Hardware und Software“ und dem „Zurückgewinnen digitaler Souveränität“ gesprochen wird (Cle18).

Auch die Übernahme von Kuka durch chinesische Investoren zeigt beispielhaft, dass die Eingrenzung des Begriffs „technologische Souveränität“ auf IKT und IT-Sicherheit wohl zu kurz greift. Weitere Technologiefelder, die für die Zukunfts- und Handlungsfähigkeit eines Staates / eines Wirtschaftsstandortes relevant, wenn nicht sogar existentiell sind, können z. B. Biotechnik (Lebensmittelversorgung), Bionik, Energie (z. B. Speicherung), Geodaten oder Pharmazie (Medikamente) sein. Eigentlich kann man „digitale Souveränität“ als einen Spezialfall „technologischer Souveränität“ einordnen, der speziell den Umgang mit Daten und ihrer Verarbeitung sowie ihre Kommunikation adressiert. Insbesondere schließt digitale Souveränität auch das Individuum als Adressaten („mediale Souveränität“) ein.

Überträgt man den Begriff „Souverän“ auf Technologien heißt „technologische Souveränität“ nichts anderes, als dass „man“ bezüglich einer Technologie eigenständig handeln und entscheiden kann, und vor allem, dass man die letzte Entscheidungsgewalt hat.

Vor dem Hintergrund der engen internationalen Vernetzung und Abhängigkeiten, angefangen von der Wissenschaft, über den Rohstoffhandel bis hin zu Produktion, wirft das die Frage auf, inwieweit derartige technologische Souveränität überhaupt erreichbar ist, bzw. welche Ziele man mit technologischer Souveränität eigentlich erreichen will. In welchen Branchen und Technologiefeldern welcher Grad an technologischer Souveränität angestrebt wird bzw. sogar erforderlich ist, hängt davon ab, wie umfassend man die Wertschöpfungskette abdecken will und welche Rolle individuelle Protagonisten in der Wertschöpfungskette einnehmen. Letztlich bedarf es übergeordneter strategischer und politischer Entscheidungen.



Abb. 1: Zusammenhang verschiedener Formen von Souveränität

Im Folgenden konzentriert sich das Positionspapier auf Technologien der IKT, die inzwischen als existenziell einzustufen sind. Im Zuge der Digitalisierung beeinflusst die IKT letztlich alle Branchen und durchzieht zunehmend auch alle Bereiche unseres Lebens. Zugleich stellt das Positionspapier immer wieder auch Bezüge zu anderen Technologiefeldern her und diskutiert „technologische Souveränität“ in einem breiteren Kontext.

3. Aspekte „technologischer Souveränität“

Um sich dem zu nähern, was der Begriff „technologische Souveränität“ umfassen könnte, bedarf es, mehrere Aspekte quasi als Dimensionen in Beziehung zueinander zu setzen (Abb. 2). Auch der Bitkom hat in seiner jüngsten Stellungnahme zur digitalen Souveränität verschiedene Dimensionen zur Konkretisierung identifiziert (Bit19).

Eine Dimension stellt die Technologie selbst, strukturiert in Technologiefelder dar. Die Definition eines „Technologiefeldes“ erweist sich als nicht so einfach wie der Begriff zunächst suggerieren mag. Die Schwierigkeit ergibt sich aus der Abgrenzung zwischen Technologiefeld, Branche und Anwendungsfeld. Während bei einem Technologiefeld die Technologie als solche im Vordergrund steht, kann eine Technologie durchaus für sehr unterschiedliche Anwendungen in verschiedenen Branchen eingesetzt werden. Die Technologien der IKT sind hier augenfällig. Die Branchen und Anwendungen gehen daher als zweite Dimension in die Betrachtung ein. Die dritte Dimension erfasst die Anforderungen an Souveränität. Was man durch die Fähigkeit zu souveränem Handeln erreichen kann, hängt wesentlich davon ab, mit welcher Aufgabenstellung man konfrontiert ist. Geht es um den Aufbau von Wissen, Ausbildung, die Fähigkeit zur Produktion oder zum Betrieb, oder auch „nur“ um die Anwendung durch den Endverbraucher? Daher wird die Bedeutung des Begriffs „Souveränität“ entlang einer generalisierten Wertschöpfungskette konkretisiert.

Im Folgenden werden die Begriffe der drei Dimensionen näher definiert. Für die Erfassung von Technologiefeldern wird eine Systematik vorgeschlagen. Darauf aufbauend werden die drei Dimensionen in Beziehung zueinander gesetzt und Kriterien zur Identifikation und Bewertung der für souveränes Handeln relevanten Technologiefelder vorgeschlagen.

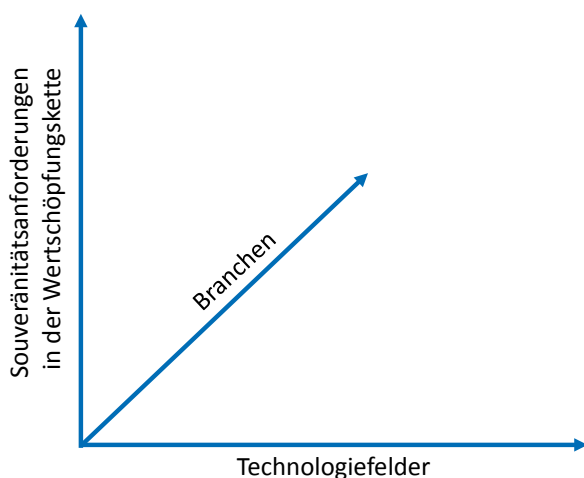


Abb. 2: Betrachtete Dimensionen der Souveränität

3.1 Dimension „Branchen“

Unternehmen werden als einer Branche zugehörig benannt, wenn diese weitgehend substituierbare Produkte und Dienstleistungen herstellen (Eng00). Für die Branchenzuordnung existieren verschiedene Einteilungen. So unterscheidet sich beispielsweise die Einteilung von Statista deutlich von der Einteilung des BMWi (siehe Anhang B). Im Folgenden werden als eine Dimension der Bewertung die vom BMWi definierten Branchen herangezogen.

Der Begriff „Anwendungsfeld“ beschreibt Bereiche, in denen „etwas“, hier also eine bestimmte Technologie, Anwendung findet. Damit sind Branchen und Anwendungsfelder nicht notwendigerweise deckungsgleich, da z. B. die Bürokommunikation als Anwendung der IT in vielen verschiedenen Branchen zum Einsatz kommt. Die IT ist somit zunächst einmal eine Technologie und, wie noch ausgeführt werden wird, aber auch Teil eines Technologiefeldes. Zugleich wird die IT aber auch als Teil der IKT als eigene Branche geführt.

Eine separate Strukturierung in Anwendungsfelder erscheint vor dem Hintergrund, dass Anwendungen ein Merkmal von Branchen sind, nicht erforderlich (kein Erkenntnisgewinn), zumal im Gegensatz zu Anwendungsfeldern für Branchen umfangreiche Wirtschaftsdaten vorliegen, die wesentliche Kriterien bei der Beurteilung der wirtschaftlichen Relevanz darstellen.

3.2 Dimension „Technologiefelder“

Die Anforderungen und die Ausgestaltung technologischer Souveränität soll in ausgewählten Technologiefeldern analysiert und dargestellt werden. Für den Begriff „Technologiefeld“ existiert keine einheitliche, allgemeingültige Definition, wodurch sich in der Literatur unterschiedliche Einteilungen mit variierender Granularität finden (Mai15) (GK16) (CP00). Als erster Orientierungspunkt dient daher die Einteilung der OECD, nicht zuletzt da es sich um eine internationale normative Referenz handelt (OEC07). Die inzwischen zwölf Jahre alte Einteilung ist mit den im weiteren Kontext der Elektrotechnik relevanten Technologiefeldern sehr abstrakt:

- 1.2 . . . Computer and information sciences
- 2.2 . . . Electrical engineering, electronics engineering, information engineering
- 2.5 . . . Materials engineering
- 2.6 . . . Medical engineering
- 2.10 . . . Nano-technology
- 5.8 . . . Media and communications

Einen Anhaltspunkt zur Konkretisierung gibt die Weiterentwicklung der Klassifikation von Technologie in Basis-, Zukunfts-, Schrittmacher-, Schlüssel- und Hochtechnologie (Zim07). Aktuell erscheinen daraus u. a. die folgenden Technologie(felder) relevant:

- Optronik
- Optische Technologien
- Laser
- Elektronik
- Mikroelektronik
- ...

Schon diese Auswahl zeigt eine sehr detaillierte Einteilung. Gesucht wird deshalb eine Einteilung, die zur Zuordnung von Technologien hinreichend konkret ist, aber dennoch die Anzahl der Technologiefelder überschaubar lässt. Auch sollen Technologiefelder eine längere zeitliche Konstanz aufweisen.

Im Hinblick auf die Zielsetzung „Technologische Souveränität“ wird der Ansatz verfolgt, Technologiefelder von Branchen respektive Anwendungsbereichen zu trennen. In Abgrenzung hierzu stehen bei der Einordnung in Technologiefelder essenzielle technische Funktionen und die zur Realisierung erforderlichen „Technologien“ im Vordergrund, die dann in vielen auch sehr unterschiedlichen Anwendungen und Branchen zum Einsatz kommen können. Das Diagramm in Abb. 3 soll diesen Zusammenhang visualisieren. Je nach Abstraktionsgrad der Technologiefelder könnte der Begriff IKT sowohl eine Branche als auch ein Technologiefeld benennen.

Was sind aber nun geeignete Kriterien, um ein Technologiefeld zu definieren und zu identifizieren?

Als Startpunkt wurde die fachliche Untergliederung der Fachgesellschaften GI, VDE und VDI herangezogen (siehe Anhang A), die sich inhaltlich eher an Technologien als an

Branchen orientieren. Daraus lassen sich auf relativ abstrakter Ebene Technologiefelder ableiten, die zwar Ähnlichkeiten zu Branchen und Anwendungen aufweisen, aber doch technologisch „gedacht“ sind. Für eine technologische Bewertung erscheint diese Ebene jedoch als zu abstrakt.

Letztlich entstehen technische Systeme dadurch, dass bestimmte Funktionalitäten schrittweise zu immer komplexeren Systemen zusammengebaut werden, um bestimmte Aufgaben zu erfüllen. In diesem Papier bezeichnet der Begriff „Technologiefeld“ technische Systeme, die bestimmte Kernfunktionen ausführen. Beispielsweise geht es in der IKT im Kern darum, Informationen zu transportieren, diese aufzubereiten, zu speichern und zu verarbeiten.

Zur Realisierung dieser Funktionalitäten eignen sich verschiedene (Schlüssel-)Technologien. Während sich Kernfunktionen über der Zeit nicht ändern (z. B. Datentransport), verändern sich die zur Realisierung genutzten Technologien über der Zeit sehr wohl. Im Hinblick auf „technologische Souveränität“ geht es also darum, die zur Realisierung einer Funktion mit den erforderlichen Leistungsdaten, Kosten etc. erforderlichen aktuellen „Schlüsseltechnologien“ einsetzen zu können. Schlüsseltechnologien werden hier als solche Technologien verstanden, mit denen wirtschaftlich relevante neue technische Funktionalitäten möglich werden oder bestehende technische Funktionen besonders wirtschaftlich realisiert werden können. Im Sinne eines souveränen Handelns ist damit nicht notwendigerweise eine revolutionäre Art und Weise verbunden, die einen „Innovationsschub weit über die Grenzen eines einzelnen Wirtschaftsbereichs hinaus auslöst“ (Wik19a). Dieses Verständnis von Schlüsseltechnologie hat zur Folge, dass es auch von der Anwendung und Zielsetzung abhängen kann, ob eine Technologie eine Schlüsseltechnologie ist oder nicht.

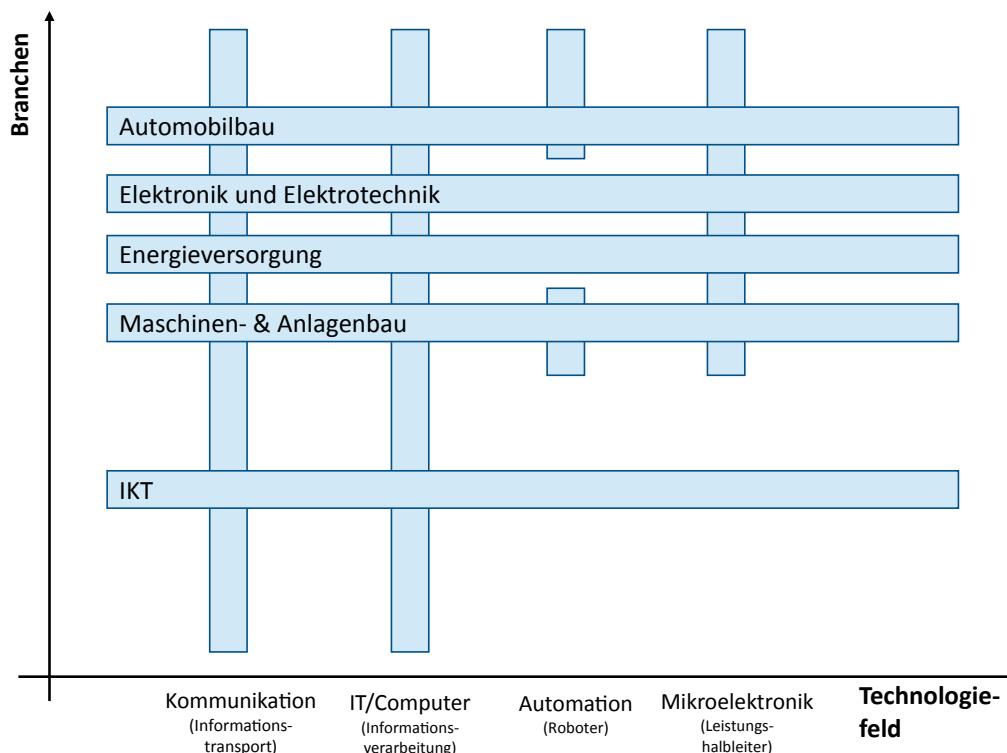


Abb. 3: Darstellung, in welchen Branchen / Anwendungen Technologiefelder eine erhebliche Rolle spielen

Technologiefelder	Systembereiche (Funktionen)	Schlüssel - Technologien	Technologiefelder	Systembereiche (Funktionen)	Schlüssel - Technologien
Informations- und Kommunikationstechnik (IKT)	Kommunikation	5G	Digitale Plattformen	Handelsplattformen	Geschäftsmodelle
		Schwarmkommunikation			Identitätsmanagement
		optische Kommunikation			e-payment
	IT / Computer	Quantencomputer		Transaktionssysteme	Authentifizierungsverfahren
		Kleinstcomputer (IoT)			
		Höchstleistungscomputer			Software as a Service
	Sicherheit	autom. Sicherheitsanalysen	Serviceplattformen	Micro-Services	
		Verschlüsselung			
		Blockchain			
Mikroelektronik	SoC	mixed signal integration	Energie	Erzeugung	Kleinstkraftwerke
		Energieminimierung			Biokraftwerke
	Leistungselektronik	SiC / GaN		Verteilung	smart networks
	Neuronale Netze	Prozessorarchitekturen		Speicherung	Batterietechnik
TPU / GPU Architekturen		Gaskonversion			
Software	Entwicklung	automatische Verifikation	Automation	Industrieautomation	digitaler Zwilling
		Virtualisierung			
	Simulation	Schwachstellenanalyse		Robotik / autonome Systeme	Mensch-Roboter-Interaktion
		digitaler Zwilling			kognitive Erkennung
	MMI	Sprach-/Gesichts/Gestenerkennung		Mess- und Regelungstechnik	Sensorik
gedankliche Steuerung					
Künstliche Intelligenz	maschinelles Lernen	deep learning	Medizintechnik	Diagnostik	Messtechnik
		kognitive Systeme			
		Trainingsverfahren			
	Empfehlungs- / Expertensysteme			Behandlung	OP-Technik
					Bio-Sensorik / -Aktuatoren
	Datenanalyse	Datenaggregation und -Speicherung		Pflegetechnik	Micro-Roboter (Blutbahn)

Abb. 4: Identifizierte Technologiefelder, sowie relevante Systembereiche innerhalb des jeweiligen Technologiefeldes. Die aufgeführten Schlüsseltechnologien sind nur als Beispiele zu verstehen und beanspruchen keine vollständige und umfassende Erfassung aller Schlüsseltechnologien.

Abb. 4 stellt exemplarisch aus Sicht der ITG relevante Technologiefelder zusammen mit den Systembereichen / Kernfunktionen dar. Die darunter aufgeführten Schlüsseltechnologien sind ebenfalls als beispielhaft zu verstehen. In der Analyse zeigt sich auch, dass eine einzelne Schlüsseltechnologie bzw. auch Schlüsselfunktionalität verschiedenen Technologiefeldern zugeordnet werden kann.

3.3 Bewertung der Relevanz von Technologiefeldern

Wie bewertet man nun ein Technologiefeld hinsichtlich seiner Relevanz im Hinblick auf „technologische Souveränität“? Welche Schlüsseltechnologien muss man in welcher Wertschöpfungstiefe „souverän“ beherrschen, um eine bestimmte Funktion oder Anwendung in einer bestimmten Branche realisieren zu können? Beispielsweise könnte ein neuartiges Material einen extrem sensiblen taktilen Sensor für Roboter ermöglichen. Hat man Anwendungen, die nur mit diesem Sensor realisierbar sind, so wäre die Fähigkeit zum souveränen Einsatz dieser Technologie anzustreben. Besteht hingegen nur an Anwendungen Bedarf, die mit konventionellen Greifern realisiert werden können, so ist die Relevanz

dieser speziellen Sensortechnik in Bezug auf souveränes Handeln gering.

Es geht also nicht darum, Technologien um ihrer selbst willen souverän zu beherrschen, sondern Technologien wegen wirtschaftlicher, gesellschaftlicher und politischer Relevanz souverän nutzen zu können.

Um „relevante“ Technologiefelder zu identifizieren, sind entsprechende Klassifikationskriterien erforderlich, die am Thema „Technologische Souveränität“ bzw. an deren Zielsetzung ausgerichtet sind. Naturgemäß geht es oft vorrangig um den Erhalt der wirtschaftlichen Leistungsfähigkeit. Zugleich zeigt die Diskussion zur digitalen Souveränität aber auch, dass Sicherheitsaspekte eine wesentliche Rolle spielen sollten, wenn es um die Identifikation „relevanter“ Technologiefelder geht. Sicherheit meint hier nicht nur IT-Sicherheit, sondern auch funktionale Sicherheit und, viel weiter gefasst, letztlich nationale Sicherheit. Auch sollten Fragen der Versorgungssicherheit (inkl. Lebensmittel, Gesundheit), der Nachhaltigkeit (z. B. CO₂-Neutralität, Umweltschutz) sowie relevante gesellschaftliche Aspekte bei der Analyse von Technologiefeldern aus der Perspektive „technologischer Souveränität“ nicht fehlen – also übergeordnete politische Zielsetzungen. Zur Bewertung der Relevanz von Technologiefeldern unter dem Blickwinkel „technologischer Souveränität“ werden folgende Kriterien vorgeschlagen:

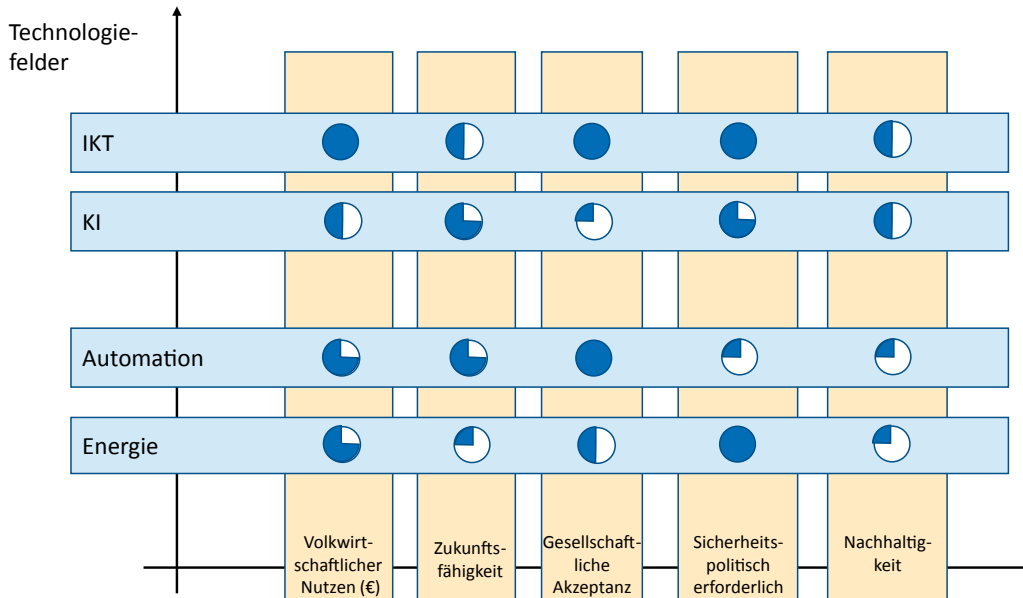


Abb. 5: Gesamtheitliche IST-Bewertung von Technologiefeldern. Die dargestellte Bewertung ist exemplarisch ohne empirische Grundlage

▪ Volkswirtschaftlicher Nutzen

- Aggregierte Wirtschaftsleistung der Branchen, für die das Technologiefeld relevant ist. Ein Technologiefeld wird nicht für die gesamte Wirtschaftsleistung verantwortlich sein, sodass eine prozentuale Gewichtung denkbar ist, die sozusagen die „Hebelwirkung“ des Technologiefeldes für die Branche abbildet.
- Die aktuelle Wachstumsrate des Umsatzes in einer Branche kann ein Anhaltspunkt sein, der jedoch nur bereits wirtschaftlich genutzte Technologiefelder erfasst. Die Zuordnung zu einem bestimmten Technologiefeld ist nur sehr bedingt möglich.
- Einfließen sollte auch, welche Lebensdauer man dem Technologiefeld aus heutiger Sicht zumisst.
- Potential für neue Geschäftsmodelle: Gerade im Zeitalter der Digitalisierung stellen neue, digitale Technologien nutzende Geschäftsmodelle etablierte Wertschöpfungsketten infrage bzw. ersetzen diese. Daher erscheint es notwendig, Technologiefelder auch nach dem Disruptionspotential für neue (digitale) Geschäftsmodelle zu bewerten. Der Einstieg von Apple in Bezahlendienste ist nur ein Beispiel dafür, wie die Finanzbranche von branchenfremden Marktakteuren Konkurrenz erhält.

▪ Zukunftsfähigkeit

- Die Innovationsfähigkeit stellt die Basis für die zukünftige Wettbewerbsfähigkeit dar. Daher bietet sich als Kriterium das erwartete (geschätzte) Wirtschaftspotential an, das sich aus der Nutzung des Technologiefeldes in weiteren wirtschaftlich interessanten Anwendungsfeldern entwickeln könnte.
- Der Reifegrad einer Technologie („technological readiness level“ (Wik19b)) hilft bei der Beurteilung des Zeitrahmens, bis eine Technologie wirtschaftlich erfolgreich eingesetzt werden kann. In einem sehr frühen Stadium der Technologieentwicklung ist es zumeist

noch einfacher, Souveränität zu erlangen, als wenn eine Technologie entwickelt und im Markt etabliert ist.

▪ Gesellschaftliche Akzeptanz

- Eine Technologie, die keinerlei gesellschaftliche Akzeptanz findet, ist unter Umständen unter volkswirtschaftlichen Aspekten ungeeignet, bzw. erhöht die Gesamtkosten (z. B. Atomkraft).

▪ Sicherheitspolitische Notwendigkeit

- Innen- und / oder außenpolitische Relevanz unabhängig von Wirtschaft und Branche
- Für eine Technologie kann aus Gesichtspunkten der Sicherheit (Cyberangriffe, geheimdienstliche und / oder militärische Aspekte) die Notwendigkeit für souveräne Handlungsfähigkeit bestehen. Dies ist letztlich eine politische Entscheidung.
- Souveräne Handlungsfähigkeit in einem Technologiefeld kann aber auch relevant zur Gewährleistung der Versorgung sein (Strom, Logistik, ...).

▪ Nachhaltigkeit

- Auch wenn dieser Aspekt nicht unmittelbar wirtschaftliche Aspekte adressiert, so sollte er heute aus Verantwortung vor der Umwelt immer berücksichtigt werden. Außerdem reduziert sparsamer, nachhaltiger Umgang mit Ressourcen (inkl. Wiederverwertung) auch die Abhängigkeit von internationalen, zuweilen auch monopolistischen, Lieferanten.

Abb. 5 veranschaulicht, wie die Relevanz eines Technologiefeldes aus der Bewertung entlang der vorstehenden Kriterien abgeleitet werden kann. Ein zunehmender Füllgrad eines Harvey Balls zeigt eine wachsende Bedeutung eines Kriteriums für ein Technologiefeld an. Beispielsweise ist aktuell der volkswirtschaftliche Nutzen der IKT sehr hoch, allerdings ist derzeit unsere Fähigkeit die zukünftige Entwicklung der IKT international maßgeblich zu gestalten nur sehr beschränkt.

Dargestellt ist eine Betrachtung des IST-Zustandes, genauso gut lässt sich mit diesem Ansatz auch ein gewünschter Endzustand (Soll) darstellen. Es sei explizit darauf hingewiesen, dass die hier dargestellte Bewertung rein exemplarischen Charakter hat, da sie auf keiner empirischen Analyse basiert.

Ein wesentlicher Aspekt lässt sich aus dieser Zusammenstellung nicht erkennen: Die Bedeutung und die Fähigkeit, in komplexen Systemen zu denken, diese zu konzipieren, zu bauen und zu betreiben.

„Die Erfolgsgeschichte vieler Teile der deutschen Systemindustrie hing und hängt von der Kompetenz der deutschen Zulieferindustrie bei Entwurf und Fertigung kundenspezifischer Mikro- und Nanoelektronik ab. Die darauf aufbauende Kombination von Hardware und Software ermöglicht Alleinstellungsmerkmale und Premiumvorteile.“ (MR15)

Auch anhand der IKT lässt sich das verdeutlichen. Um die IKT in anderen Branchen zielgerichtet einsetzen zu können, bedarf es detaillierter Kenntnisse der spezifischen Anforderungen und des Kontextes (Domain-Wissen). Beispielsweise entstehen in der Energiewirtschaft im Übergang von großen zentralen Kraftwerken zu sehr vielen Kleinkraftwerken (Windräder, Solaranlagen, Biomasse, ...) neue Anforderungen an die Kommunikation zwischen sehr, sehr vielen Netzelementen (Generator, Verteilung, Verbraucher). Zukunftsträchtige Lösungen können letztlich nur durch das Zusammenbringen des Domain-Wissens aus der Energiewirtschaft und der IKT entwickelt werden.

Auch in der Entwicklung der Industrieautomation (Industrie 4.0) fließt Domain-Wissen sehr unterschiedlicher Technologiefelder und Fachdisziplinen zusammen, u. a. klassisches Produktionswissen, IKT, KI und Mikroelektronik. Das immer wichtiger werdende interdisziplinäre Zusammenspiel über Technologiefeldgrenzen hinweg kann aber nur erfolgreich sein, wenn in allen beteiligten Technologiefeldern ausreichende Souveränität vorhanden ist.

3.4 Dimension „Anforderungen an Souveränität“

Was bedeutet „souveränes Handeln“ konkret im Hinblick auf Technologien? Ein produzierendes Unternehmen hat ganz andere Anforderungen an souveräne Handlungsfähigkeit als ein Netzbetreiber oder der Endverbraucher, oder auch der Staat mit seinen Institutionen und seiner Verantwortung für den gesellschaftlichen Zusammenhalt. Daher bietet es sich an, Anforderungen an „souveränes Handeln“ entlang einer verallgemeinerten Wertschöpfungskette zu gliedern.

Betrachtet man die Wertschöpfungskette, so haben die Beteiligten je nach Stufe in der Wertschöpfungskette sehr unterschiedliche Anforderungen an den Zugang und den Umgang mit Technologien. Hinzu kommt, dass Marktteilnehmer je nach Rolle und Aufgabenstellung die Anforderungen an technologische Souveränität für einzelne Abschnitte der Wertschöpfungskette unterschiedlich bewerten. So wird in der Kommunikationstechnik ein Netzbetreiber andere Vorstellungen haben als ein Netzausrüster oder der Nutzer. Als für die Souveränität relevante Rollen von Marktteilnehmern werden in einem einfachen Modell berücksichtigt:

- Kunde / Endverbraucher
- Betreiber / Dienstleister / Händler
- Hersteller
- Forschung / Ausbildung

Da sich diese Rollen gut den Stufen der verallgemeinerten Wertschöpfungskette zuordnen lassen, werden die Rollen von Marktteilnehmern bei der Betrachtung der Anforderungen an die technologische Souveränität nicht separat betrachtet, vielmehr wird eine Stufe der Wertschöpfungskette primär unter dem Blickwinkel der zugeordneten Rolle betrachtet. Übergreifend nehmen auch Gesellschaft und Politik als Gesetzgeber und Regulierer eigene Rollen ein. Deren Anforderungen fließen in die Bewertung der Relevanz eines Technologiefeldes ein.

Im Folgenden werden die Anforderungen und möglichen Erwartungen an eine „souveräne Handlungsfähigkeit“ entlang der Wertschöpfungskette analysiert.

Wissensmanagement, Ausbildung, Weiterbildung

Um überhaupt Zugang zu einer Technologie haben zu können, ist das Wissen um die Technologie selbst erforderlich. Es geht um den Zugang zu Informationen, Wissen, Datenbanken, Publikationen, aber auch um den Zugang zu internationalen Expertengruppen zum Gedankenaustausch. Es braucht Lehrer, die die Informationen aufbereiten und vermitteln können. Schließlich geht es nicht nur um das Erarbeiten neuen Wissens, sondern im Hinblick auf Einsatz und Nutzung einer Technologie auch um den Betrieb mit ihr realisierter Systeme und damit um Aus- und Weiterbildung. Vor dem Hintergrund, dass Technologien zum Teil sehr lange in Betrieb sein können, muss auch langfristig Zugang zu Wissen vorhanden sein, u. U. länger als ein Produkt vermarktet wird.

Unabhängig davon, wer welche Aufgaben entlang der Wertschöpfungskette tatsächlich wahrnimmt, z. B. auch ausländische Lieferanten, ist „vor Ort“ – also im Land selbst – ausreichend Expertise unabdingbar, damit man die Qualität der „Lieferung“ zumindest validieren und einordnen kann.



Abb. 6: Generalisierte Wertschöpfungskette

Wissensmanagement ist eine Grundvoraussetzung, um in einem Technologiefeld agieren zu können. Jegliche Form von Souveränität unabhängig vom Technologiefeld erfordert also immer selbstbestimmten und eigenständig gestaltbaren Wissensaufbau und Wissensvermittlung.

Eine Besonderheit der IKT ist, dass auch eine kontinuierliche Vermittlung aktuellen Wissens an jeden Bürger stattfinden muss. In dem Umfang, wie jeder Bürger zwingend mit Informations- und Kommunikationstechniken umgehen muss, z. B. bei der Nutzung des Internets, zunehmend auch im Zusammenhang mit öffentlicher Verwaltung, muss hier auch Weiterbildung und Sensibilisierung bezüglich IT-Sicherheit und Datenschutz stattfinden. Die Souveränität im Wissensmanagement stellt somit eine Grundvoraussetzung dar, um dem Bürger souveränen Umgang mit der Digitalisierung zu ermöglichen.

Forschung

Zusätzlich zu den vorstehenden Ausführungen zum Wissensaufbau lebt die Forschung von Forschungsprojekten, in denen neue Erkenntnisse theoretisch und experimentell gewonnen werden. Der Zugang zu internationalen Expertengruppen und auch die enge Zusammenarbeit in internationalen Teams ist unverzichtbarer Bestandteil. Die experimentelle Seite erfordert Zugang zu Hochtechnologie aus unterschiedlichsten Bereichen, u. a. in Form von Mess- und Produktionseinrichtungen und auch Materialien / Rohstoffen. Der Zugang zu Software und Algorithmen gehört ebenso dazu, wobei gerade in der Forschungs-Community der Gedanke des „open source“ und frei verfügbare Publikationen fest verankert ist.

Souveränität im Forschungsumfeld bedeutet also vor allem den politischen Willen, bestimmte Themengebiete an Universitäten und Hochschulen zu verankern und Forschung zu diesen Themen zu fördern.

In der IKT spielt die internationale Standardisierung eine zentrale Rolle. Das Durchsetzen eigener Anforderungen, z. B. wie Prozesse zum Datenmanagement abgebildet werden, setzt fundierte Forschungsarbeiten voraus, um die Basis für international akzeptierbare technische Vorschläge zu schaffen. Wer sich nicht selbst in der Standardisierung engagiert, muss mit den von anderen darin festgeschriebenen technischen Verfahrensweisen leben. Souveräne Forschung und umfassende aktive Beteiligung in der internationalen Standardisierung sind Eckpfeiler dafür, dass spätere Produkte bestimmte Eigenschaften aufweisen – oder eben auch nicht.

Produktentwicklung

In der Entwicklung geht es vor allem darum, ein Produkt zu konzipieren, als Prototyp zu realisieren, auszutesten und zu optimieren. Bereits in der Entwicklungsphase fließen die Anforderungen aus der Produktion ein, z. B. erforderliche Materialien, Herstellbarkeit auf verfügbaren Maschinen, Verfügbarkeit von Komponenten. Um ein marktfähiges Produkt entwickeln zu können, bedarf es umfassender und vielfältiger technischer Expertise, aber auch praktischer Erfahrung, die nicht nur das Kerngebiet (z. B. Netzwerktech-

nik) umfasst, sondern auch viele andere Fachbereiche. Je komplexer ein Produkt ist, z. B. ein Auto, umso vielfältiger sind die relevanten Technologiefelder.

Die Grade möglicher Souveränität sind hier größer. So kann man sich auf Systemintegration fokussieren, indem ein Großteil der Komponenten von Dritten entwickelt und zugeliefert wird, wie es z. B. heute in der Automobilbranche üblich ist. Genauso kann man die Strategie einer hohen Wertschöpfungstiefe verfolgen, möglichst das gesamte Produkt selbst herzustellen, womit das Unternehmen an Souveränität, also an selbstbestimmtem Handeln gewinnt. So baut Bosch in Dresden eine eigene Chipfabrik, um „die Schlüsseltechnologie in eigenen Händen zu halten ...“ (Dew17). Zugleich nehmen die Anforderungen an die Produktentwicklung zu. Es braucht eine gewisse „Souveränität“ in vielen Technologiefeldern, um ein Produkt erfolgreich entwickeln zu können.

Als aktuelles Beispiel eignet sich die Batterieentwicklung, die man als Schlüsseltechnologie für die Elektromobilität betrachten kann. Ohne ausreichende Expertise und Zugang zu dieser Technologie ist die Entwicklung wettbewerbsfähiger Elektroautos, aber auch anderen Anwendungen, die von effizienten Batterien profitieren könnten, nur sehr eingeschränkt möglich.

Neben der Entwicklung der Hardware ist kaum mehr ein System ohne Software zu finden. Doch die Software-Stacks sind heute sehr umfangreich und bestehen aus vielen Bibliotheken unterschiedlichsten Ursprungs. Es ist kaum mehr möglich, alle Software-Ebenen selbst zu entwickeln, zumindest ist das unter marktwirtschaftlichen Gesichtspunkten kaum realisierbar. Und auch in der Software-Entwicklung sind umfangreiche Entwicklungswerkzeuge erforderlich. Souveräne Handlungsfähigkeit bedeutet hier Zugang zu den entsprechenden Entwicklungswerkzeugen und Software-Bibliotheken, aber auch mit den Werkzeugen und den Methoden der Software-Entwicklung vertraute Experten. Gerade weil Software zu einer essentiellen Komponente moderner Systeme geworden ist, erfordern die mit der Software einhergehenden Sicherheitsanforderungen hohe Aufmerksamkeit. Ein hohes Maß an Souveränität in der Software-Entwicklung stärkt die Gewährleistung von Sicherheitsanforderungen.

Produktion

Für die Herstellung eines Produktes ist der Zugang zu Produktionsmaschinen, Materialien und Komponenten erforderlich. Zur Qualitätssicherung sind zum Teil umfangreiche Prüfeinrichtungen, Maschinen und ggf. auch weitere Materialien notwendig. Zu berücksichtigen ist auch, dass ohne eine ausgereifte Logistik heute kaum mehr erfolgreich produziert werden kann. Schließlich müssen auch entsprechend qualifizierte Mitarbeiter verfügbar sein. Gerade bei komplexeren Produkten beschränken sich die Anforderungen an Infrastruktur, Material und Wissen nicht auf ein Technologiefeld.

Zu berücksichtigen ist auch, dass in machen Bereichen die technischen Anforderungen so hoch sind, beispielsweise in der Chipfertigung oder in der Fertigung von

Präzisionsoptiken, dass es weltweit nur sehr wenige Lieferanten für die Produktions- und Prüfmaschinen gibt.

Somit erscheint das Erreichen umfassender „technologischer Souveränität“ (nationale Autarkie) bezogen auf die Produktion eines komplexeren Produktes nicht oder nur sehr schwer erreichbar. Bezogen auf die IKT ist immer wieder davon zu lesen, dass man in der Lage sein sollte, Kernkomponenten der Kommunikationsinfrastruktur selbst herstellen zu können. Die Konsequenzen sind weitreichend, da ja nicht nur der Router oder die Basisstation zusammengebaut werden müssen, sondern diese aus vielen Komponenten, insbesondere Chips besteht. Souveränität in der Produktion des Routers würde somit auch Souveränität in der Chipfertigung, inklusive der Fertigungsmaschinen und der Prüfeinrichtungen umfassen. Neben diesen technologischen Fragen sprechen bei vielen Produkten auch die hohe Komplexität und der damit erforderliche Entwicklungsaufwand und resultierend der wirtschaftliche Zwang zur Nutzung von Skaleneffekten gegen die Sinnhaftigkeit nationaler Autarkie.

Welcher Grad an Souveränität, an selbstbestimmtem Handeln und Entscheiden, ist bei der Produktion von Produkten / Geräten sinnvoll und möglich? Da man nicht um Kooperationen und Zulieferungen ausländischer Unternehmen umhinkommt, steht unmittelbar die Frage im Raum, wie man nicht nur die Zuverlässigkeit (Qualitätssicherung ist ein etablierter Prozessschritt), sondern gerade, wenn IKT involviert ist, sofort auch die Vertrauenswürdigkeit verifizieren kann. Die Diskussion um die Vertrauenswürdigkeit von Huawei bei der Ausrüstung von 5G-Netzen zeigt, wie sensibel dieser Aspekt ist. Der Austausch der IT-Hardware in staatlichen Organisationen in China durch nationale Produkte bis 2022 (Han19) zeigt, dass Souveränität über die eigene Infrastruktur auch für andere Volkswirtschaften eine sehr hohe Bedeutung hat. Die Verfügbarkeit wird bereits heute bis zu einem gewissen Grad über die „Dual Supplier“-Strategie abgesichert.

Betrieb

Der Betrieb einer technischen Einrichtung / technischen Infrastruktur erfordert umfangreiches Wissen über das Betriebsverhalten eines Gerätes / einer Infrastruktur. Der Anspruch besteht darin, durch souveränes Handeln den gewünschten Betriebszustand einer Infrastruktur / eines Netzes herzustellen, aufrecht zu erhalten und bei Störungen wiederherzustellen.

Die Wartung erfordert ein tiefgehendes Verständnis der Komponenten und in aller Regel kennt nur der Hersteller alle Details und kann sehr tiefliegende Probleme beheben. Damit geht aber auch einher, dass der Hersteller Zugang zu sehr sensiblen operativen Daten bekommen kann.

Souveräner Betrieb beinhaltet auch den Aspekt der Resilienz. Wie kann Infrastruktur so aufgebaut werden, dass im Störfall nicht die gesamte Infrastruktur lahmgelegt wird? Hiermit ist am Beispiel von Kommunikationsnetzen nicht nur gemeint, dass man Inhalte über zwei völlig unterschiedliche Strecken routen kann, sondern dass für die

alternative Kommunikationsstrecke andere Übertragungstechnologien zum Einsatz kommen.

Ein weiterer Aspekt des Betriebes von Systemen ist die Rückkopplung in die Entwicklung; Fließen Erfahrungen aus dem Betrieb in die Weiterentwicklung von Produkten bzw. in die Konzeption der Nachfolgegenerationen ein, so lassen sich sehr viel bessere Produkte bauen.

Im Bereich staatlichen Handelns gelten für den Betrieb technischer Systeme oftmals besondere Anforderungen, wie sie mit hoheitlichen Aufgaben oder der Gewährleistung innerer und äußerer Sicherheit einhergehen.

Nutzung

Zunächst müssen alle Bürger über eine gewisse Souveränität im Umgang mit digitalen Infrastrukturen und Daten verfügen. Dies setzt entsprechende Kenntnisse voraus. Als Bürger besteht ferner ein hohes Interesse daran, was wo mit den persönlichen Daten passiert.

Auf Seiten professioneller Nutzung kann souveräne Handlungsfähigkeit erforderlich sein. Diese unterscheidet sich aber deutlich je nach Bedarfsträger. In der Wirtschaft gibt es eine große und von der jeweiligen Geschäftstätigkeit abhängige Spannweite. Die öffentliche Hand, insbesondere Sicherheitsbehörden, haben ein vitales Interesse an hoch-sicherer Datenkommunikation. IT-Geräte müssen ebenfalls absolut sicher betrieben werden können. Im Verteidigungsbereich ist weitgehende Autarkie z. B. in Bezug auf die Kommunikation erforderlich.

Erneuerung

Schließlich entsprechen in manchen Anwendungsbereichen die Investitionszyklen nicht den technischen Entwicklungszyklen. Anlagen werden wesentlich länger betrieben als technischer Support vom Hersteller bereitgestellt wird. Beispiele sind Infrastrukturen in öffentlicher Hand, Prozessanlagen, oder auch Militärtechnik. Souveränität bedeutet in diesem Kontext, über Investitionszyklen hinweg unabhängig von technischen Entwicklungszyklen entscheiden zu können

4. Ausprägungen technologischer Souveränität

Wie sich bereits in der Betrachtung der Wertschöpfungskette abzeichnet, gibt es verschiedene Ausprägungen von Souveränität (MRB18). Diese beschreiben, was letztlich mit Souveränität erreicht werden soll. Ausgehend von den Anforderungen aus der Wertschöpfungskette wird vorgeschlagen, folgende Formen der Souveränität zu unterscheiden.

- **Wissenssouveränität**
 - Gewährleistet den Zugang zu Wissen und die Fähigkeit, Wissen zu vermitteln
 - Souveränität in der Aufbereitung von Informationen und Wissen
 - Verfügbarkeit von Experten / Lehrern, die über das Wissen verfügen
 - Fähigkeit zur Bewertung von Technologien
- **Forschungssouveränität**
 - Selbstbestimmte Entscheidung zu Forschungsthemen (aufgreifen, verfolgen, fördern, ...)
 - Selbstbestimmter Zugang zu internationalen Forschergruppen mit freiem Informationsaustausch
 - Zugang zu aktuellen Technologien, Komponenten und Rohstoffen, um z. B. Experimente / Messungen u. ä. durchführen zu können
- **Infrastruktursouveränität**
 - Fähigkeit, das Funktionieren komplexer Systeme erfassen, bewerten und beeinflussen zu können
 - Fähigkeit, technische Infrastrukturen vertrauenswürdig herzustellen, oder zumindest ihre Vertrauenswürdigkeit zu validieren
 - Fähigkeit, technische Infrastrukturen so zu betreiben, dass darauf angebotene Dienste vertrauenswürdig sind
- **Datensouveränität**
 - Entscheidungsfreiheit und Selbstbestimmung über die Verwendung „eigener“ Daten; „eigen“ meint die Daten, die entweder einer Firma gehören oder persönliche Daten
 - Eine absolut vertrauliche Verwendung persönlicher Daten muss gewährleistet sein.
 - Jeder muss die vollständige Kontrolle darüber haben, wer welche Daten hat.
 - Anwendungen erfassen nur diejenigen Daten, die nachvollziehbar für das Funktionieren eines Dienstes unabdingbar sind. Freiwilliges Erfassen weitergehender Daten schließt nicht von der Nutzung des Dienstes aus.
 - Gewährleistung der Privatsphäre (privacy by design)
- **Transparenzsouveränität:**
 - Möglichkeit, Ursprünge und Begründungen für Entscheidungen und Handlungsempfehlungen autonomer Systeme / KI und Assistenten nachzuvollziehen und diese gegebenenfalls durch menschliches Eingreifen zu beeinflussen

- **Entwicklungssouveränität**

Um ein Produkt entwickeln zu können, sind bereits in der Entwicklungsphase nicht nur umfassende Kenntnisse über die spätere Produktion erforderlich, sondern bereits Fertigungsfähigkeiten, z. B. für Prototypen, als auch Produktionsschritte zu testen. Somit dürften die meisten Aspekte der Produktionssouveränität auch für die Entwicklungssouveränität relevant sein. Zusätzliche Aspekte sind

- Selbstbestimmtes Entscheiden über Konzept, Ausgestaltung und schließlich Umsetzung eines Produktes
- Zugang zu Produktionsmitteln
 - Produktionssouveränität

Zentral für Produktentwicklungen sind detaillierte Kenntnisse der Marktanforderungen, also der zukünftigen Betreiber und Nutzer, die über die Frage „wie etwas funktionieren soll“ wesentliche Auswirkungen auf die Technik haben. Ohne umfassenden Zugang zu (vertrauenswürdigen) Software-Werkzeugen ist heute keine Entwicklung (Hardware und Software) möglich. Je mehr die Software Teil der Wertschöpfung wird, umso mehr besteht auch die Notwendigkeit, in der Lage zu sein, Software auf die eigenen spezifischen Anforderungen anzupassen.

- **Produktionssouveränität**

Um ein Produkt herstellen zu können, sind gerade für komplexe Produkte (z. B. Auto) sehr viele unterschiedliche Voraussetzungen im Sinne von „Souveränität“ erforderlich. Zum Beispiel sind auf dem Weg zum fertigen Auto sehr viele Komponenten zu produzieren, die wiederum unter dem Blickwinkel der Produktionssouveränität zu betrachten sind.

- Zugang zu Rohstoffen
- Fähigkeit, Rohstoffe zu verarbeiten (→ Produktion)
- Zugang zu Komponenten
- Zugang zu Produktionsanlagen und Ausrüstungsgütern
- Betrieb von Produktionsinfrastrukturen (→ Betrieb, Infrastruktur, Daten, Transparenz)

- **Plattformsouveränität**

- Fähigkeit, marktrelevante Plattformen aufzubauen und zu betreiben, einschließlich der erforderlichen Finanztransaktionssysteme; ggf. kann das bedeuten, dass durch Regulierungsvorgaben nicht-lineare Skalierungseffekte digitaler Plattformen so kanalisiert werden, dass Plattformen in einen fairen Wettbewerb treten können.

- **Betriebssouveränität**

- Verfügbarkeit von für den Betrieb erforderlichen spezifischen Geräten (Hardware und Software), insbesondere, wenn diese so nur von einem / sehr wenigen Herstellern produziert werden (Exportkontrolle ist ein wirksames Mittel, die Handlungsfähigkeit eines Staates / Wirtschaft zu „steuern“)

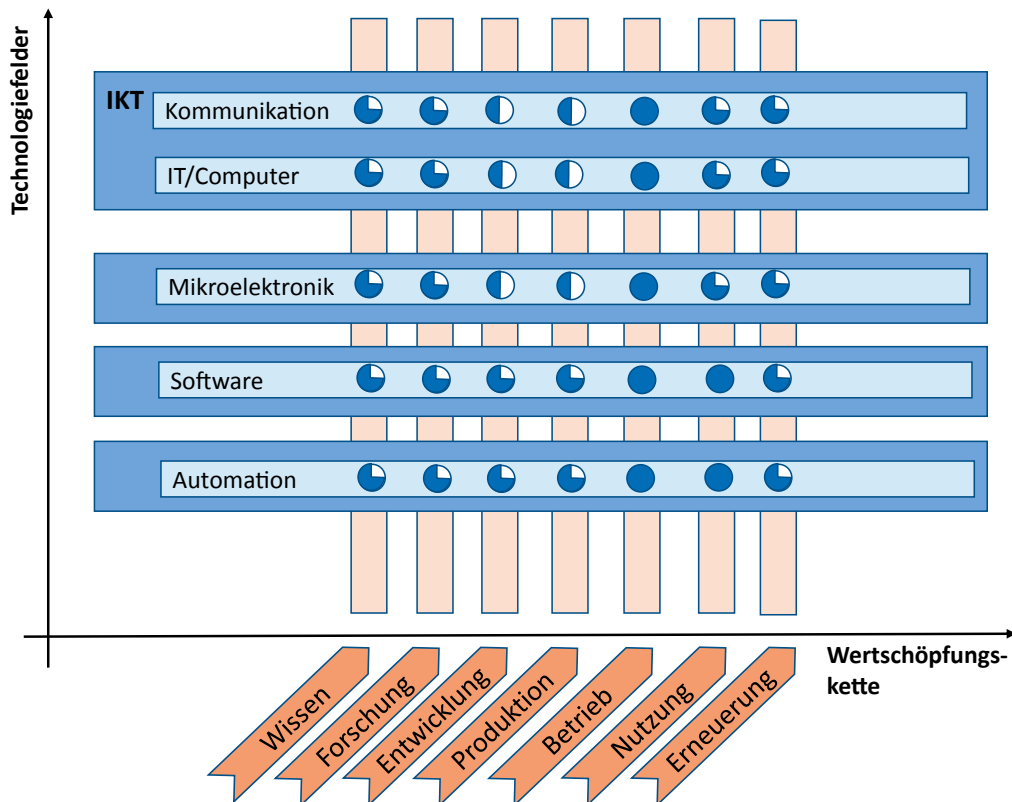


Abb. 7: Beispielhafte Grade technologischer Souveränität für Technologiefelder entlang der Wertschöpfungskette

- Kenntnisse zur vollständigen Einrichtung, Steuerung und Störungsbehebung

▪ Mediensouveränität

- Digitale Bildung als gesellschaftliche Aufgabe

4.1 Grade souveränen Handelns

Ganz unabhängig davon, welche konkreten Anforderungen an Souveränität gestellt werden, lassen sich übergeordnete und von Rollen und Technologien unabhängige Grade der Souveränität definieren (und als Harvey-Bälle visualisieren):

1. Alles selbst wissen, entwickeln, herstellen und / oder betreiben (weitgehende Autarkie). (Kreis voll)
2. Das Wissen, die Fähigkeiten und die Komponenten anderer nur punktuell nutzen. Man behält die vollständige Kontrolle über das gesamte System und alle Bestandteile. (Kreis $\frac{3}{4}$ gefüllt)
3. Das Wissen, die Fähigkeiten und die Komponenten Dritter werden in erheblichem Umfang eingesetzt und man verlässt sich auf deren zuverlässiges Funktionieren. Dies schließt auch den partiellen Betrieb und die Wartung von Komponenten ein. (Kreis halb gefüllt)
4. Der Systemaufbau und die Systemintegration, inkl. Auswahl und Fertigung der Komponenten, wird Dritten überlassen. Der Betrieb liegt noch in den eigenen Händen, ist allerdings ohne Support des Systemintegrators nicht (umfassend) möglich. Im Wesentlichen liegt nur das zum Betrieb nötige Wissen vor. (Kreis $\frac{1}{4}$ gefüllt)
5. Es gibt keine eigene Kompetenz; Fertigung und Betrieb wird vollständig anderen überlassen. (Kreis leer)

Die Nutzung ist bereits als Teil der Wertschöpfungskette mit ihren spezifischen Anforderungen an Souveränität erfasst worden. Wo man bislang selbstverständlich von einer vollständig souveränen Nutzung von Produkten ausging, kann sich dies im Zuge der Digitalisierung ändern. Beispielsweise kann der Hersteller eines Smartphones heute durchaus in die Funktionsfähigkeit eines Gerätes eingreifen, die Souveränität des Nutzers in der Nutzung seines Smartphones wird dadurch zu einem gewissen Grad eingeschränkt. Daher erscheint es notwendig auch der Nutzung verschiedene Souveränitätsgrade zuzuordnen. Souveränität kann so für die identifizierten Technologiefelder entlang der Wertschöpfungskette bewertbar gemacht werden. Dies ist in Abb. 7 exemplarisch dargestellt. Die hier gezeigten Bewertungssymbole sind beispielhaft zu verstehen. Belastbare Aussagen erfordern eine umfassende systematische Abfrage. Eine solche Abfrage erlaubt auch, sowohl den Ist- als auch den Soll-Zustand zu erfassen, womit erkennbar wird, wo besonders großer Handlungsbedarf besteht.

Bei genauerer Analyse zeigt sich, dass es nahezu unmöglich ist, für ein ganzes Technologiefeld übergreifend einheitliche Souveränitätsanforderungen entlang der Wertschöpfungskette zu formulieren. So wird das Technologiefeld IKT unter dem Blickwinkel 5G völlig anders zu bewerten sein als beispielsweise unter dem Blickwinkel Quantencomputer. Im folgenden Abschnitt wird dies anhand von zwei Beispielen verdeutlicht. Zugleich zeigt das Diagramm, dass sich mit Hilfe der vorgeschlagenen Systematisierung Technologiefelder auf unterschiedlichen Abstraktionsebenen bis auf der Ebene von Schlüsseltechnologien bewerten lassen.

4.2 Beispielhafte Anwendung der Systematik

Die Eignung der vorgestellten Systematik zur Ableitung von Positionen und Anforderungen im Hinblick auf „technologische Souveränität“ wird an zwei Beispielen aus dem Kontext der ITG vorgestellt. Bereits bei der Analyse der Souveränitätsarten entlang der Wertschöpfungskette zeichnete sich ab, dass die Bewertung eines Technologiefeldes nur unter dem Blickwinkel einer konkreten Anwendung / Anwendungsbereichs möglich ist. Erst mit Hilfe des spezifischen Domain-Wissens, also des Wissens um die Anwendung, lässt sich eine Aussage zu den tatsächlichen Anforderungen an technologische Souveränität machen. Letztlich kann die Systematik somit sowohl auf eine spezifische (Schlüssel-)Technologie als auch ein Technologiefeld angewendet werden.

Als Beispiele wurde die Schlüsseltechnologie 5G und das Technologiefeld KI ausgewählt, die in einem vielfältigen Zusammenhang stehen. 5G ermöglicht beispielsweise mit seinen hohen Datenraten die Übertragung hochauflösender Video-Streams. Während die systematische Auswertung der Nutzung durch Menschen heute fast nicht mehr möglich ist, stellt die heutige KI Verfahren bereit, die über vergleichende Muster-Erkennung und selbstlernende Algorithmen die Erkennung von spezifischen Merkmalen möglich machen, sodass der Konsument seinen Interessen gemäß darauf hingewiesen werden kann.

An dieser Stelle sei nochmals ausdrücklich darauf hingewiesen, dass die Bewertungen indikativ sind, da diese von Experten erstellt wurden, aber nicht auf einer systematischen, statistisch belastbaren Studie beruhen.

4.2.1 Beispiel 5G (Schlüsseltechnologie)

5G ist die „5. Generation der Mobilfunksysteme“, die zurzeit weltweit eingeführt wird. Zur Einordnung ein kurzer Abriss:

- 1G = Analogtechnik, für Sprache
- 2G = Digitaltechnik, für Sprache, SMS und langsame Datendienste (GSM, GPRS, Edge)
- 3G = Digitaltechnik, für Sprache, SMS und Internetzugang (UMTS)
- 4G = Digitaltechnik, für Internetzugang, Sprache, SMS und Video (LTE)
- 5G = Digitaltechnik, Cloud-native, für Video, Internetzugang, Sprache, SMS und für die höchst unterschiedlichen Anforderungen des „Internets der Dinge“ im Kontext der Digitalisierung über alle Branchen und Lebensbereiche hinweg.

5G verfügt über drei Kerneigenschaften, die anwendungsspezifisch miteinander kombiniert werden können:

- Extrem große Kapazität und Geschwindigkeit der Datenübertragung (bis 10 Gbit/s pro Funkzelle)
- Echtzeitfähigkeit (bis hinunter zu 1 ms Latenzzeit der Datenübertragung) und hohe Zuverlässigkeit in der Datenübertragung („five nines“ 99,999% bei 1 ms Latenz, und „six nines“ 99,9999% bei größeren Latenzzeiten)

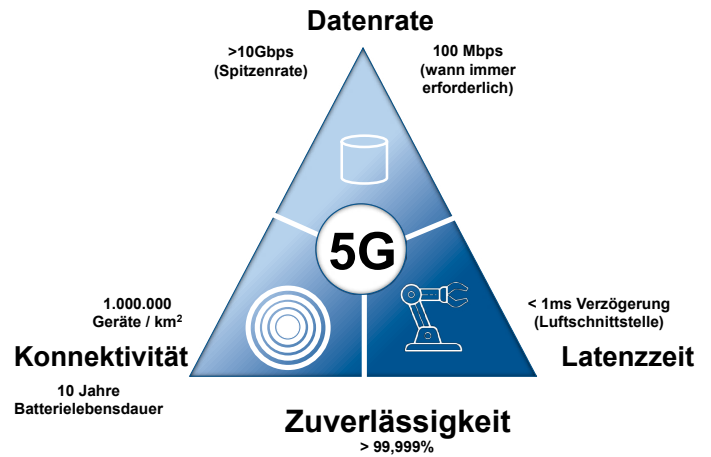


Abb. 8: Kerneigenschaften von 5G

- Konnektivität zur Anbindung sehr großer Mengen an IoT-Geräten (bis zu 1 Million Geräte pro km²).

Neben diesen funktionalen Eigenschaften ermöglicht 5G mit seiner modernen, auf die Cloud-Technologie ausgelegten Systemarchitektur sog. Network Slicing, also den Aufbau virtueller Sondernetze mit anwendungsspezifischen Eigenschaften auf gemeinsamen physischen Infrastrukturen. Die 5G-Architektur ist auch für die Kombination von 5G mit Edge Computing ausgelegt, um damit die IT-Funktionen Verarbeitung und Speicherung von Daten physisch nahe am Anwender bereitzustellen, was je nach Anwendung mit geringerer Latenzzeit sowie Sicherheit und Effizienzgewinnen durch lokale Verarbeitung/Vorverarbeitung und Datenhaltung weitere Potentiale eröffnet.

Mit diesen Charakteristika ermöglicht 5G eine Vielzahl neuer Anwendungen für verschiedene Benutzergruppen. Einige Beispiele:

- Unternehmen können 5G etwa für Prozesssteuerung und -überwachung in Echtzeit, zur Objektlokalisierung oder zur hochzuverlässigen, drahtlosen Maschinenkommunikation verwenden und damit die Produktivität durch Flexibilisierung und vernetzte Produktionsprozesse steigern.
- Mit autonomen Fahrzeugen und Drohnen sind visuelle Inspektionen von Bauwerken und Anlagen mittels hochauflösender Bilder und Videos möglich und Servicekräfte können bei ihrer Arbeit durch AR/VR-Anwendungen unterstützt werden.
- Es wird möglich, massenhaft Umwelt- und Zustandsdaten durch Sensoren zu erfassen und zur weiteren Auswertung bereitzustellen.
- In Verkehr und Logistik sind Unterstützung autonomen Fahrens (z. B. Platooning oder automatisiertes Einparken bei LKW-Flotten) sowie Automatisierung von Güterbahnhöfen und Seehäfen vielversprechende Anwendungsgebiete.

In Deutschland sind Aufbau und Betrieb von 5G-Netzen nicht nur Mobilfunkbetreibern vorbehalten, sondern Unternehmen können für ihre Standorte spezifische, lokal nutzbare Frequenzen erhalten, damit dem Charakter von 5G als innovativem Produktionsmittel optimal Rechnung getragen werden kann.

Das Thema 5G findet derzeit im Hinblick auf technologische Souveränität breite öffentliche Aufmerksamkeit, nicht nur wegen der vielfältigen Möglichkeiten und Erwartungen, die damit verbunden sind, sondern auch vor dem Hintergrund, inwieweit welche internationalen Ausrüster ausreichend vertrauenswürdig für eine kritische Infrastruktur sind.

Neben dem System als Ganzem mit seinen Möglichkeiten und dem 5G-Netz müssen auch die 5G-Endgeräte gezielt betrachtet werden: Die genannten 5G-Anwendungen können nur dann nutzbringend eingesetzt werden, wenn die „Dinge“ im Internet der Dinge mittels maßgeschneidert

leistungsfähiger, zuverlässiger und wirtschaftlicher Endgeräte (z. B. in den „Dingen“ integrierter Modems oder Chips) über das 5G-Netz mit den zugehörigen Anwendungsplattformen im Hintergrund verbunden sind.

In der folgenden Tabelle werden die Souveränitätsanforderungen entlang der Wertschöpfungskette für die Schlüsseltechnologie 5G insgesamt formuliert. Soweit erforderlich wird dabei zwischen dem 5G-Netz und den 5G-Kommunikationskomponenten auf Anwenderseite („5G-Endgerät/Modem/...“) differenziert.

WERTSCHÖPFUNGSKETTE	GRAD DER ERFORDERLICHEN SOUVERÄNITÄT	
Ausbildung / Weiterbildung	5,0	In der entstehenden digitalisierten Welt ist im Industrieland Deutschland das Wissen um die IKT im Allgemeinen und damit auch um 5G zwingend erforderlich. Der spezifische Fokus und Tiefgang des Wissens hängt naturgemäß von der Rolle des Einzelnen in der Gesellschaft, im Unternehmen etc. ab.
Wissenssouveränität	5	5G ist eine Schlüsseltechnologie für völlig neue Anwendungsfelder in Industrie und Gesellschaft. Diese können nur erschlossen werden, wenn wir selbst über das Wissen verfügen, wie die Technologie im Detail funktioniert und welche Potentiale sich damit eröffnen.
Forschung	5,0	5G wird in den nächsten Jahren im Zuge der Digitalisierung Wirtschaft und Gesellschaft durchdringen und zu einem zentralen „Nervensystem“ werden. Die heute verfügbare 5G-Technologie wird dabei noch über viele Jahre hinweg eine substantielle Weiterentwicklung erfahren; das Verständnis der Anwendungsmöglichkeiten und konkreten Anwendungen von 5G steht dabei erst am Anfang. Damit wir die Innovationspotentiale von 5G in Wirtschaft und Gesellschaft entdecken, nutzen und in Wettbewerbsvorteile für unsere Unternehmen umsetzen können, müssen wir sowohl bei der Technologieforschung als auch interdisziplinär bei der Anwendungsforschung vorne dabei sein. Der Zeitlinie bisheriger Netzgenerationen folgend ist ab ca. 2030 mit der Nachfolgeneration 6G zu rechnen, die nur auf einer soliden Forschungsposition in 5G heraus maßgeblich mitgestaltet werden kann.
Wissenssouveränität (s. o.)	5	Fachwissen zu 5G, seiner Technologieentwicklung und seiner Anwendung ist für die beteiligten Fachleute in Lehre, F&E und Anwendung/Betrieb erforderlich.
Forschungssouveränität	5	Um bei der Anwendung von 5G nachhaltig vorne dabei zu sein und Erfahrungen aus der Anwendung von 5G in Industrie und Wirtschaft in die Weiterentwicklung und weltweite Standardisierung von 5G einbringen zu können, ist eine breite und tiefe, besonders auch interdisziplinäre, Forschung mit entsprechenden Ressourcen erforderlich. Bisherige Netzgenerationen haben zudem gezeigt, dass gemeinsame Forschungsprojekte zwischen Industrie und Hochschulen ein wichtiger Erfolgsfaktor in den frühen Phasen der Technologieentwicklung sind.

WERTSCHÖPFUNGSKETTE		GRAD DER ERFORDERLICHEN SOUVERÄNITÄT	
Produktentwicklung		3,0	Aufgrund des Zukunftspotentials für viele Anwendungsbereiche besteht die Notwendigkeit Produkte für eine 5G-Infrastruktur selbst entwickeln zu können. Es ist unrealistisch, hierfür die Produkte vollständig angefangen von den Chips zu entwickeln, der Zukauf von Komponenten ist unumgänglich. Zugleich muss man umfassendes technisches Wissen über das gesamte System haben, um anwendungsspezifisch Systeme entwickeln zu können (Industrie 4.0, autonomes Fahren)
Wissenssouveränität (s. o.)		4	Fachwissen zu 5G, seiner Technologieentwicklung und seiner Anwendung/ seinem Betrieb ist für die beteiligten Fachleute erforderlich.
Entwicklungssouveränität		3	5G-Infrastruktur kann aufgrund der Komplexität und der notwendigen immensen F&E-Vorleistungen nur von international agierenden Unternehmen bereitgestellt werden. Daher müssen wir die Kompetenzen besitzen, wichtige Teile der Produktentwicklung abdecken zu können; es ist aber nicht erforderlich, dass komplette 5G-Systeme in Deutschland entwickelt werden können. Sinngemäß das Gleiche gilt für die 5G-Komponenten in den Endgeräten/über 5G angebundene IoT-Devices etc. Für die optimale Nutzung von 5G kann es allerdings notwendig sein, dass die Entwicklung von Anwendungen/mit 5G ausgestatteten branchenspezifischen Produkten und Lösungen vollständig beherrscht wird.
Produktionssouveränität		2	5G-Komponenten müssen nicht in Deutschland produziert werden, sofern der ausreichende Zugang zu den Netzelementen für den Aufbau der Netze und den 5G-Kommunikationskomponenten in Endgeräten/Anwendersystemen gewährleistet ist (s. u.). Daher sind auch FuE-Aspekte wie Fertigungseinführung etc. nicht vorrangig.
Betriebssouveränität		3	Erfahrungen und Innovationen aus dem Betrieb von Systemen und 5G-Anwendungen müssen in 5G-Produkte eingebracht werden können.
Produktion		2,4	5G-Komponenten müssen nicht in Deutschland produziert werden, sofern der ausreichende Zugang zu den Netzelementen für den Aufbau der Netze und den 5G-Kommunikationskomponenten in Endgeräten/Anwendersystemen gewährleistet ist.
Rohstoffe	Zugang	1	Keine Bedeutung
	Verarbeitung → Produktionssouveränität	1	Keine Bedeutung
Komponenten	Zugang	5	Falls eine eigene Produktion angestrebt wird, muss der Zugang zu Bauteilen gewährleistet sein. Netzkomponenten müssen gesichert aus vertrauenswürdiger Produktion verfügbar sein: Funktionalität und Leistungsfähigkeit, Wirtschaftlichkeit, Qualität, Sicherheit (insbesondere hinsichtlich Cybersecurity) und Liefervolumina. Gleiches gilt für 5G-Endgeräte/Modems zur Integration in Anwendersysteme, wobei hier je nach Anwendung die Integration von 5G-Komponenten und Anwendungskomponenten in speziellen Chips Vorteile bringen kann (Beispiel IoT-Sensorik).
	eigene Herstellung → Produktionssouveränität	3	Kann anwendungsabhängig für Endgeräte/erforderlich sein. Ansonsten ist der Zugang zu fertigen Netzelementen und Endgeräten/Modems wichtig, nicht die Produktion.

WERTSCHÖPFUNGSKETTE		GRAD DER ERFORDERLICHEN SOUVERÄNITÄT
Produktionsanlagen / Ausrüstung	Zugang	2 Für Netzelemente nur relevant, sofern (s. u.) der Aufbau eigener Produktionskapazitäten erforderlich werden sollte. Für hochintegrierte Anwendungsgeräte (s. o.) kann die Verfügbarkeit geeigneter Produktionsmittel Voraussetzung für die Wettbewerbsfähigkeit der mit 5G angebotenen Produkte sein. Beurteilung im Anwendungskontext.
	→ Wissenssouveränität	3 Wissen erforderlich, um die Situation beurteilen zu können, und – falls erforderlich – den Aufbau eigener Produktionskapazitäten planen und umsetzen zu können (geopolitische Aspekte).
Betrieb von Produktionsinfrastrukturen	→ Betriebssouveränität	2 Relevant nur insofern eigene Produktion notwendig wird (s. o.)
Betrieb (Anbieter, B2B)		4,8 Aufgrund des Zukunftspotentials für viele Anwendungsbereiche besteht die Notwendigkeit Produkte für eine 5G-Infrastruktur selbst entwickeln zu können. Es ist unrealistisch, hierfür die Produkte vollständig angefangen von den Chips zu entwickeln, der Zukauf von Komponenten ist unumgänglich. Zugleich muss man umfassendes technisches Wissen über das gesamte System haben, um anwendungsspezifisch Systeme entwickeln zu können (Industrie 4.0, autonomes Fahren)
	Betriebssouveränität	5 Für die Nutzung von 5G-Systemen muss der Betrieb durch kompetente Firmen und geschultes, vertrauenswürdigen Personal in jedem Fall sichergestellt sein. Das gilt sowohl für die Betreiber öffentlicher 5G-Netze als auch für Inhouse-Netze in Unternehmen und Behörden, ggf. mit aaS-Komponenten. Die Rückkopplung von Erfahrungen aus dem Betrieb in die Weiterentwicklung von 5G und in die Forschung ist ein entscheidendes Element zur Erhaltung der Forschungssouveränität.
	Infrastruktursouveränität	5 Aufbau, Ausbau, Betrieb und Optimierung von 5G-Netzinfrastrukturen müssen eigenständig souverän beherrscht werden, sowohl von den Betreibern öffentlicher Netze wie von Organisationen/Unternehmen für lokale Firmen-/Campusnetze.
	Transparenzsouveränität	5 Unabdingbar für Akzeptanz. Dabei spielt das Vertrauen in die 5G-Systeme, besonders das Netz, für die Gesellschaft und nutzende Institutionen/Unternehmen eine entscheidende Rolle: Ist 5G vertrauenswürdig, sind Datenübertragungen über 5G abhörsicher, nicht korrumpierbar, nicht durch Externe (Kriminelle, Staaten, ausländische Unternehmen) abschalt- oder fälschbar? Daher ist Transparenz über die 5G-Wertschöpfungskette für alle beteiligten Akteure essentiell.
	Datensouveränität	5 Unabdingbar für die Souveränität von Unternehmen/Organisationen und für das Land. Wegen der erwarteten Durchdringung von 5G ein entscheidender Faktor. Umfasst alle Aspekte der Cybersecurity, dabei besonders die Sicherheit der mit 5G übertragenen Daten selbst und die gesicherte Verfügbarkeit der 5G-Systeme (Netz und Endgeräte/Modems) gegen evtl. Sabotage.

WERTSCHÖPFUNGSKETTE	GRAD DER ERFORDERLICHEN SOUVERÄNITÄT	
Plattformsouveränität	4	5G-Netze werden sich zu Plattformen für vielfältige digitale Transaktionen im B2B- und B2C-Bereich entwickeln. Daher ist es wichtig, dass entsprechende Ökosysteme souverän entwickelt und betrieben werden können.
Nutzung (Konsument / Gesellschaft)		3,7
Datensouveränität	4	Wichtig für die Souveränität des Einzelnen, von Unternehmen/Organisationen und für das Land. Wegen der erwarteten Durchdringung von 5G noch weitaus relevanter als heute.
Transparenzsouveränität	4	Notwendig für Akzeptanz von 5G in der Breite. Dabei spielt das Vertrauen in die 5G-Systeme für die Gesellschaft und die Individuen eine große Rolle (s. o.): Ist 5G vertrauenswürdig, abhörsicher, nicht korrumpierbar, nicht durch Externe (Kriminelle, Staaten, ausländische Unternehmen) abschalt- oder fälschbar? Außerdem ist Transparenz bzgl. der Strahlenbelastung durch 5G wesentlich, damit Ausbau und Betrieb von 5G-Systemen nicht durch sachlich unbegründete Proteste behindert werden.
Mediensouveränität	3	Wissen um kompetente Nutzung ist in der Breite erforderlich (s. o.)
Ersatz	3,0	Die Migration von auf bisherigen Kommunikationstechnologien aufgebauten Anwendersystemen auf die Nutzung von 5G erfordert Fachkenntnis, Zugang zu entsprechenden Daten/Informationen und entsprechende rechtliche/vertragliche Freiheitsgrade. Gleiches wird in ferner Zukunft bei der Migration von 5G auf 6G gelten.

4.2.2 Beispiel KI / Data Science (Technologiefeld)

Als ein weiteres Beispiel wird das Technologiefeld KI näher betrachtet. Zwar hat KI durch die enorme aktuelle Dynamik den Charakter einer Schlüsseltechnologie, als die sie an anderer Stelle auch definiert wird. KI selbst ist jedoch schon mehrere Jahrzehnte alt, während sich die innerhalb der KI genutzten Technologien über die Zeit deutlich gewandelt haben.

Dieses Technologiefeld erhält aktuell große öffentliche und politische Aufmerksamkeit, indem z. B. autonome Systeme die Öffentlichkeit mit ihrer Leistungsfähigkeit verblüffen und zum anderen die Politik aufgefordert wird, noch stärker als bisher in diese Technologien zu investieren. Andere Nationen investieren sehr hohe Summen in die Forschung und kritische Stimmen vertreten die Auffassung, dass „der Zug für uns abgefahren sei“.

Für eine nähere Betrachtung ist zunächst zu klären, was damit gemeint ist. Innerhalb des Sammelbegriffs KI erfährt der Bereich des „maschinellen Lernens“ (ML) derzeit breitere praktische Relevanz. Hierbei geht es darum, dass Maschinen in der Lage sind, selbständig in Daten Muster zu erkennen und zu „lernen“, um darauf aufbauend neue Informationen zu bewerten, klassifizieren oder auch neue Lösungen zu entwickeln. Der Begriff „deep learning“ (DL) bezeichnet einen Spezialfall innerhalb des ML. Dieser Bereich dürfte heute die höchste praktische Relevanz haben, da diese Verfahren bereits in einer Vielzahl von Anwendungen eingesetzt werden. Das Anwendungsportfolio wächst beständig und die hinter „deep learning“ stehenden Verfahren werden immer ausgefeilter. Daher wird „deep learning“ in diesem Papier auch als Schlüsseltechnologie geführt. Technisch basiert „deep learning“ auf neuronalen Netzen mit zum Teil sehr vielen Schichten. Allerdings gibt es sehr unterschiedliche Netzstrukturen, Regeln zur Verknüpfung der Neuronen (Knoten) und funktionalen Eigenschaften der Neuronen. „convolutional neural networks“ (CNN) erweisen sich aktuell als sehr vielseitige und leistungsfähige Netzstruktur für Klassifikationsaufgaben. Damit ein neuronales Netz Eingangsdaten analysieren und klassifizieren kann, muss das Netz mit passenden Musterdaten trainiert werden. Die Daten müssen die zu lösende Aufgabe hinreichend charakterisieren und die zu klassifizierenden Ereignisse in ausreichender statistischer Relevanz beinhalten.

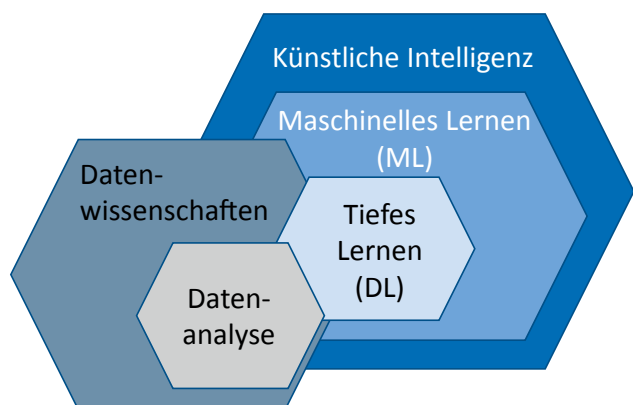


Abb. 9: Zusammenhang von Künstlicher Intelligenz und maschinellem Lernen

Zu einer Herausforderung kann es werden, wenn sehr viele klassifizierte Daten (labeled data) für das Training erforderlich sind.

Im Kontext des maschinellen Lernens fällt immer auch der Begriff „data analytics“ / „data science“. Die in diesem Wissenschaftsgebiet angewandten Methoden haben aber nur zum Teil einen Bezug zum „machine learning“, da in der Datenanalyse häufig klassische mathematisch-statistische Verfahren Anwendung finden. Den Zusammenhang veranschaulicht Abb. 9. Aufgrund der hohen Bedeutung der Datenanalyse im Zusammenhang mit „deep learning“ ordnet dieses Papier aber den Bereich der Datenwissenschaften („data science“) dem Technologiefeld KI zu.

Die Datenanalyse ist sowohl Voraussetzung und als auch eine Anwendung für „deep learning“. Für das Training von Netzen sind größere Datenmengen aufzubereiten. Zum anderen lassen sich mit Hilfe neuronaler Netze große unstrukturierte Datenmengen auch analysieren („big data“ / „smart data analytics“). Breitere praktische Anwendung finden die technischen Konzepte des „deep learning“ heute beispielsweise unter anderem bei der Analyse von Nutzungsdaten, um Vorhersagen über zukünftige Nutzungen treffen zu können. Eine Datenanalyse wird zunehmend auch zur Optimierung von Prozessen (Logistik, Fertigung, ...) eingesetzt, vorausgesetzt, hier können Betriebsdaten in ausreichender Menge und Qualität bereitgestellt werden.

Hinter dem Begriff „machine learning“ (ML) oder auch „deep learning“ (DL) steht zunächst einmal nur eine abstrakte Algorithmik, man könnte es auch „Werkzeugkasten“ nennen. Das Potential dieser Verfahren erschließt sich nur in der Anwendung auf konkrete Aufgabenstellungen. Aber nicht jedes neuronale Netz eignet sich gleichermaßen gut. Nur wenn Zielsetzung, Anforderungen und Rahmenbedingungen bekannt und definiert sind, kann diese Tool-Box auch zielführend eingesetzt werden. Sind die spezifischen Rahmenbedingungen identifiziert und definiert, kann ein passendes neuronales Netz entwickelt und ein geeignetes Training konzipiert werden. Zur Auswahl und Konfiguration eines „deep learning“-Verfahrens / eines neuronalen Netzes ist also spezifisches Domain-Wissen unabdingbar. Welche Aussagen werden als Ergebnis erwartet, welche Eingangsdaten und welche Trainingsdaten stehen zur Verfügung? Für die Entwicklung eines geeigneten Netzes ist es erforderlich, genau zu verstehen, was die Algorithmen zu leisten imstande sind – und was nicht. Beispielsweise können CNNs nur diejenigen Ereignisse zuverlässig klassifizieren, die in ausreichender statistischer Relevanz im Trainingsdatensatz vorhanden sind. Die Verfügbarkeit möglichst umfangreicher relevanter Trainingsdaten spielt somit eine zentrale Rolle in der Entwicklung und Anwendung von „machine learning“-Verfahren. Auch ist zu berücksichtigen, dass die Klassifizierung nur mit einer gewissen statistischen Wahrscheinlichkeit korrekt ist. „False positive“-Entscheidungen eines „machine learning“-Verfahrens können unter Umständen gravierende Folgen haben, genauso wie nicht erkannte Ereignisse, z. B. beim autonomen Fahren.

Für die exemplarische Anwendung der vorgeschlagenen Methodik wird das Technologiefeld KI für Anwendungen im Bereich von Industrie 4.0 / Automatisierung betrachtet.

Anwendungsbeispiele von „machine learning“ im Kontext von Industrie 4.0 sind:

- **Prozessoptimierung**
 - Analyse von Prozessdaten und daraus abgeleitet z. B. Optimierung von Fertigungsprozessen
 - Adaptive Regelungen komplexer Maschinen, Fertigungsstraßen
- **Vorausschauende Wartung**
 - Analyse von Betriebsdaten, um daraus abzuleiten, wann ein Bauteil gewartet bzw. ausgetauscht werden muss. Wartung / Bauteilaustausch erfolgt nur dann, wenn es auch wirklich erforderlich ist.
- **Intelligente Sensoren**, z. B.
 - Klassifikation von Bauteilen direkt in der Kamera
- **Autonome Fahrzeuge in der Logistik**
- **Bildklassifizierung** (mensenähnliche Bildverarbeitung)
 - Z.B. bei der Interaktion von Mensch und Roboter in der gemeinsamen Montage.
- **Intelligentes Angebotswesen**
 - Z.B. Konfiguration komplexer Maschinen mit hoher Flexibilität (Losgröße1)

Von erheblicher Bedeutung ist, dass sich durch diese Verfahren auch die Geschäftsgrundlage grundlegend verändern kann. Ein plakatives Beispiel ist die vorausschauende Wartung oder „predictive maintenance“, wo bei Einsatz dieser Verfahren der Verkauf regelmäßiger Inspektionen und Wartungen nicht mehr funktioniert. Zugleich verändern Plattformen Wertschöpfungsketten. Das Anbieten von Diensten anstelle von Maschinen wird eine wesentlich größere Geschäftsrelevanz bekommen. Letztlich muss auch bei KI-Systemen die Technik ganz konventionell unter wirtschaftlichen Gesichtspunkten optimiert werden.

Im Folgenden werden die Souveränitätsanforderungen entlang der Wertschöpfungskette für KI / deep learning unter dem Blickwinkel der Anwendung „Industrieautomation“ formuliert.

WERTSCHÖPFUNGSKETTE	GRAD DER ERFORDERLICHEN SOUVERÄNITÄT	
Ausbildung / Weiterbildung	5,0	Selbstlernende Systeme, Verfahren des machine learnings / deep learnings werden bald allgegenwärtig sein. Jeder wird damit direkt oder indirekt konfrontiert sein. Um solche Verfahren professionell nutzen zu können, ist sowohl umfangreiches Wissen über die Funktions- und Wirkungsweise als auch über die Anwendungsmöglichkeiten selbst notwendig. Da das Wirken von ML/DL-Verfahren zumeist nicht als solches erkennbar ist, erwächst die Notwendigkeit, über Nutzungskonventionen und Transparenz gesellschaftliche Akzeptanz zu befördern. Gerade weil es im Maschinenbau keine natürliche Schnittmenge zur KI gibt, ist die Ausbildung besonders wichtig.
Wissenssouveränität	5	Ohne eigenes Wissen kann die Technologie weder angewendet noch weiterentwickelt werden. Auch eine Bewertung ist ohne eigenes Wissen nicht möglich.
Forschung	5,0	Bei Datenwissenschaften und Verfahren der künstlichen Intelligenz erleben wir derzeit eine sehr hohe Entwicklungsdynamik. Das Thema hat politische Bedeutung, da es als Wettbewerbsmerkmal eingesetzt wird (China, USA). Deutschland verfügt im Maschinen- und Anlagenbau über sehr viel (Domain)-Wissen, zugleich stellt die Automation einen wichtigen Wirtschaftssektor dar. Dieses gilt es gerade auch in interdisziplinären Forschungsprojekten zwischen Maschinenbau, Elektrotechnik und IT für die Entwicklung neuer Konzepte und Lösungen zu nutzen, um so die Wettbewerbsfähigkeit langfristig zu sichern.
Wissenssouveränität (s. o.)	5	Ohne umfangreiches eigenes Wissen ist keine Forschung möglich.
Forschungssouveränität	5	Forschung im Umfeld der KI kann nur im internationalen Austausch erfolgreich sein. Dafür müssen die deutschen Forschungseinrichtungen groß genug sein und über ausreichend Forschungsmittel verfügen, um mit den großen internationalen Einrichtungen mithalten zu können. Über Forschungsinhalte muss eigenständig entschieden werden können (→ Wissenssouveränität). Der Zugang zu ausreichend Trainingsdaten als auch die Möglichkeit, auf Art und Qualität der Daten Einfluss zu nehmen, werden als wichtig erachtet.
Produktentwicklung	3,5	KI ermöglicht im Bereich der Industrieautomation, neue Produkte und Services zu entwickeln. Nur die eigenständige Entwicklung von Produkten erlaubt es, (Domain)-spezifische Herausforderungen in der Anwendung von KI zu nutzen. Das Finden eigener Lösungswege stärkt die Wettbewerbsfähigkeit. Auf verfügbare KI-Verfahren zum Lösen von Teilaufgaben zurückzugreifen, erscheint ökonomisch sinnvoll.
Wissenssouveränität (s. o.)	4	s. o. unter Forschung
Entwicklungssouveränität	4	Grundkonzepte von Anwendungen (z. B. digitaler Zwilling, vorausschauende Wartung, Mensch-Maschine-Interaktion) werden international entwickelt. Die Anpassung an die eigenen spezifischen Belange muss eigenständig (souverän) möglich sein. Auch muss der Zugang zu den aktuellsten Entwicklungswerkzeugen verfügbar sein.

WERTSCHÖPFUNGSKETTE		GRAD DER ERFORDERLICHEN SOUVERÄNITÄT	
	Produktionssouveränität	3	Gerade das Wissen um das Zusammenwirken von Hardware und Software, z. B. in autonomen Systemen, ist entscheidend für das Funktionieren. Daher ist hier ein hohes Maß an Souveränität erforderlich., d. h. z. B. Zugang zu (KI-)Tools, (KI-)Komponenten und die Fähigkeit, diese vollkommen eigenständig einzusetzen und auf die Anforderungen hin weiter zu entwickeln.
	Betriebssouveränität	3	Die für die Entwicklung erforderlichen KI-Systeme und Software-Tools müssen verfügbar, vertrauenswürdig und eigenständig betreibbar sein.
Produktion		3,1	Betrachtet werden die Spezifika im Kontext des Einsatzes von KI. Somit ist sowohl der Zugang zu den Entwicklungswerkzeugen und den Daten als auch die Fähigkeit, diese für ein Produkt / Service einsetzbar zu machen, von zentraler Bedeutung. Werden KI-Systeme als Teil komplexerer Systeme eingesetzt (z. B. Roboter), so greifen neben den ergänzenden Anforderungen für die Hardware-Fertigung auch die Anforderungen, die sich aus der Interaktion von Hardware und Software ergeben.
Rohstoffe	Zugang	4	Spezifisch im Kontext KI ist der dauerhafte, unverfälschte, sichere Zugang zu Daten.
	Verarbeitung → Produktionssouveränität	1	Wissen und Befähigung, KI-Systeme für Anwendungen zu optimieren und zu betreiben (u. a. Regulierungen, Betriebssicherheit, ...)
Komponenten	Spezifische Komponenten sind z. B. intelligente Sensoren mit integrierter KI-basierter Vorverarbeitung.		
	Zugang	3	Der Zugang zu solchen Komponenten ist erforderlich, eine eigene Produktion nicht unbedingt ökonomisch sinnvoll. Allerdings muss deren Einsatz und Betrieb eigenständig möglich sein.
	eigene Herstellung → Produktionssouveränität	2	s. o.
Produktionsanlagen / Ausrüstung	Zugang	4	Zugang zu Software-Entwicklungswerkzeugen und die Fähigkeit, diese eigenständig zu nutzen, ist essentiell.
	→ Wissenssouveränität	4	s. o. unter Produktentwicklung
Betrieb von Produktions- infrastrukturen	Der Betrieb von Software ist zunächst kein Problem der Souveränität. Von Bedeutung ist, dass Software völlig eigenständig genutzt werden kann (kein talk-back zum Hersteller).		
	→ Betriebssouveränität	4	

WERTSCHÖPFUNGSKETTE	GRAD DER ERFORDERLICHEN SOUVERÄNITÄT	
Betrieb (Anbieter, B2B)	4,0	
Betriebssouveränität	3	Die Souveränitätsanforderungen an den Betrieb von KI-Systemen hängen sehr stark von der Anwendung ab. In der Produktion von Industriegütern dürften diese beispielsweise sehr hoch sein, in Consumer-Produkten eher sehr gering.
Infrastruktursouveränität	3	s. o.
Transparenzsouveränität	5	Die Nachvollziehbarkeit von Entscheidungen spielt im B2B-Umfeld eine erhebliche Rolle. Daher muss die zugrunde liegende Information zugänglich gemacht werden können, ohne über Dritte gehen zu müssen.
Datensouveränität	5	Daten spielen in der KI eine erhebliche Rolle, sei es zu Trainingszwecken oder sei es zur Analyse. Zugleich ist in den Datensätzen sehr viel spezifisches Wissen enthalten (Domain-Wissen). Dies macht es erforderlich, eigenständig Daten generieren und auswerten zu können.
Plattformsouveränität	4	KI-Systeme können auch (wesentlicher) Bestandteil von Plattformen im industriellen Umfeld sein, über die beispielsweise Services vermittelt werden.
Nutzung (Konsument / Gesellschaft)	3,0	
Datensouveränität	4	Für Unternehmen ist die Hoheit über ihre Daten sehr wichtig, ggf. sogar überlebenswichtig.
Transparenzsouveränität	4	Transparenz hat eine große Bedeutung, wenn es um die Akzeptanz von KI in der breiten Bevölkerung geht.
Mediensouveränität	1	Spielt hier eigentlich keine Rolle; ggf. jedoch dann, wenn KI z. B. eingesetzt wird, um automatisiert Nachrichtenquellen zu verifizieren.

5. Position der ITG

Aus Sicht der ITG ist es zunächst einmal wichtig, die Definition der Begriffe „technologische Souveränität“ und „Technologiefeld“ zu präzisieren und von anderen gebräuchlichen Begriffen wie „digitale Souveränität“ abzugrenzen. Für die ITG ist „technologische Souveränität“ sehr viel weiter gefasst als „digitale Souveränität“, da hiervon alle Technologiefelder, also beispielsweise auch die Biotechnologie, erfasst werden. Es gibt nicht DIE „technologische Souveränität“, sondern die Anforderungen an „technologische Souveränität“ unterscheiden sich wesentlich in Abhängigkeit von der Position in der Wertschöpfungskette. Zugleich zeichnet sich ab, dass sich grundsätzliche Anforderungen innerhalb einer Wertschöpfungsstufe nicht substantiell zwischen verschiedenen Technologiefeldern unterscheiden, wohl aber in der konkreten Ausgestaltung.

5.1 Anforderungen zur Erreichung technologischer Souveränität

Als Kernelemente von Souveränität im Bereich der ITK und damit in Beziehung stehender Technologiefelder kristallisieren sich folgende Aspekte heraus:

- Wir brauchen ein hohes Maß an Wissenssouveränität letztlich in allen wirtschaftlich bedeutsamen Technologiefeldern, insbesondere aber in den Technologiefeldern, die eine hohe Relevanz in vielen Anwendungsfeldern / Branchen haben. Dies gilt ganz besonders für die IKT, KI und Mikroelektronik. Wissen ist die Grundvoraussetzung für jedes nachfolgende Agieren. Ohne Wissenssouveränität ist keine einzige Form von Souveränität möglich. Das bedeutet vor allem frühzeitige Bildung in Schulen, Universitäten und nicht zuletzt in den Ausbildungsberufen. Derartige Bildung muss auch alle Bürger erreichen. Hierbei geht es nicht nur um gesellschaftliche Akzeptanz der auf der Technologie beruhenden Anwendungen, sondern auch darum, Interesse an einer Ausbildung in diesen Technologien zu wecken. Diese Bildung ist die Voraussetzung dafür, die Technologie auch tatsächlich eigenverantwortlich einsetzen zu können.
- Auch in der Forschung benötigen wir übergreifend ein hohes Maß an Souveränität. Auf der einen Seite müssen wir unsere Forschungsthemen eigenständig definieren können, was bereits entsprechendes Wissen voraussetzt. Zugleich müssen wir die Forschung ausreichend finanzieren, um in international relevanten Maßstäben Forschungsarbeiten bei uns durchführen zu können. Die Komplexität heutiger Technologien erfordert enge internationale Forschungsk Kooperationen. Aber auch hier können nur auf der Basis umfangreichen eigenen Wissens die eigenen Interessen gewahrt werden, z. B. konkret durch frühzeitiges Beantragen von Patenten.

- Aus dem Blickwinkel der ITG spielt Software für die Entwicklung von Produkten heute eine zentrale Rolle. Es geht sowohl um Entwicklungswerkzeuge als auch um Entwicklungsarchitekturen. So definieren die Werkzeuge den Anwendungsbereich und erzeugen eine Abhängigkeit, die bis in die Anwendung reicht (Stichwort Android: die Kernfunktionalitäten eines Android-Smartphones legt Google fest). Die Entwicklungen im Bereich KI-gestützter autonomer Systeme zeigen uns beispielsweise, dass Software-Architekturen eine wesentliche Rolle spielen. Entwicklungs- und Produktionssouveränität erfordert somit ein hohes Maß an Eigenständigkeit in der Software-Entwicklung. Und nur darüber lassen sich auch Sicherheitsinteressen wahren.
- Ohne Mikroelektronik funktioniert kein System mehr und dies wird noch ausgeprägter, wenn getrieben vom IoT-Gedanken nahezu alle Geräte vernetzt sein werden. Die Fähigkeit zu technologischer Souveränität unabhängig vom Technologiefeld setzt somit die Befähigung zu souveränem Handeln im Bereich der Mikroelektronik voraus. Neben der Fähigkeit, entsprechende Systeme entwickeln zu können, bedarf es der Fähigkeit, diese Systeme auch in nennenswertem Umfang bauen zu können, womit der Zugang zu Rohstoffen, Entwicklungswerkzeugen, Maschinen als auch die Fähigkeit zur souveränen Nutzung dieser Systeme verbunden ist.

5.2 Maßnahmen zur Entwicklung technologischer Souveränität

Aus der Relevanz eines Technologiefeldes und der identifizierten Grade an Souveränität entlang der Wertschöpfungskette lassen sich nun recht konkrete Handlungsschritte ableiten, in welchen Bereichen was zu tun ist, um die (gewünschte / erwartete) Souveränität zu realisieren.

- Die Förderung der Forschung steht vor der Herausforderung, frühzeitig die wirklich branchenübergreifend relevanten Technologiefelder und potentiellen Schlüsseltechnologien zu identifizieren, um diese auch umfassend fördern zu können.
 - Das branchenübergreifende Identifizieren relevanter Technologiefelder und darin enthaltener Schlüsseltechnologien sollte mit der vorgeschlagenen Methodik ergänzt werden.
 - Das Spiegeln des heutigen Prozesses an den tatsächlichen Souveränitätsanforderungen entlang der Wertschöpfungskette hilft hier, die richtigen Schwerpunkte zu setzen.

- Zugleich könnte es eine wirksame Unterstützung der Forschungsförderung sein, auch Programme aufzusetzen, die die Entwicklung von Lösungskonzepten für konkrete Problemstellungen zum Ziel haben, unabhängig von einer bestimmten Technologie. Dies würde die Interdisziplinarität fördern.
- Es entstehen heute immer komplexere Systeme, für deren Realisierung viele Technologiefelder und Domain-Wissen aus verschiedenen Branchen relevant sind. Forschungsprogramme sollten stärker die interdisziplinäre Zusammenarbeit in der Entwicklung von Systemen fördern.
- Ein wesentlicher Treiber der Digitalisierung ist die zum Teil radikale Veränderung der Geschäftsmodelle. Bereits in Forschungsprojekten muss dieser Aspekt berücksichtigt werden.
- Eng verbunden mit Forschung und Entwicklung ist die Standardisierung. Gerade Kommunikation funktioniert nicht ohne Standards. Aktive und koordinierte Mitwirkung an der Definition internationaler Standards und Normen gewährleistet zum Einen, dass bestimmte gewünschte Funktionsweisen darin enthalten sind, und zum Anderen, dass damit viele in die Lage versetzt werden, Geräte, Infrastrukturen etc. herzustellen und anzubieten, sodass keine isolierte Abhängigkeit entsteht. Wir brauchen strategisch ausgerichtete und politisch unterstützte Standardisierungsaktivitäten, gerade im Umfeld IKT, Software und KI. Die USA und China sind hier Treiber und bestimmen so die Ausgestaltung der Systeme.
- Die Fähigkeit, Software zu entwickeln, ist eine notwendige Voraussetzung zu technologischer Souveränität. Aber ohne spezifisches Anwendungswissen, Domain-Wissen, ist zielgerichtete und effiziente Software-Entwicklung nicht möglich. Daher sollten Forschungsprogramme so ausgelegt sein, dass diese als wichtigen Aspekt das Vermitteln und Nutzen von Domain-Wissen anderer Anwendungen / Branchen gerade in der ITK und der Software-Entwicklung beinhalten. Ganz zentral ist die Fähigkeit, in komplexen Systemen zu denken, diese zu konzipieren, zu betreiben und dabei auch Anforderungen und Erfahrungen aus der Nutzung einzubeziehen.
- Ein zielführender Ansatz können Software-Ausbildungsprogramme für Ingenieure (z. B. TH Ingolstadt) und die Einbindung der Informatik in konkrete technische Entwicklungsprojekte sein. Dieser Aspekt sollte auch in entsprechend konzipierte Förderprogramme des BMWi aufgenommen werden. Start-ups leben diese Symbiose häufig, da wegen ihrer begrenzten Mittel die Entwickler sowohl über Software-Expertise als auch über Domain-Wissen verfügen müssen.
- Im Kontext von Software-Entwicklung fördert die Unterstützung von „open source“- Communities souveräne Handlungsfähigkeit. Damit wird problematischen Entwicklungen entgegengewirkt, wo Firmen dem Markt Technologien als quasi offene Standards zur Verfügung stellen, sei es z. B. Android oder KI-Software. Der Entzug des Zugangs hierzu kann zu substantziellen Einschränkungen der Handlungsfähigkeit führen (vgl. Google Apps bei Huawei). Die Veröffentlichung des Quellcodes in diesen Communities hilft auch, Sicherheitslücken vorzubeugen bzw. solche besser zu identifizieren.
- Es besteht ein grundlegender Gegensatz zwischen Datenschutz und der Notwendigkeit, Daten möglichst vielfältig auswerten zu können. Es wird daher angeregt, neue Konzepte zu entwickeln, die nicht darauf setzen, möglichst viele Daten zentral zu erfassen und zu verarbeiten. Die Leistungsfähigkeit moderner Rechner (z. B. Smartphones) und Kommunikationsinfrastrukturen (z. B. edge computing) nutzend können Daten auch lokal aufbereitet werden. Es würde genügen, nur die Regelwerke bzw. Auswertungslogiken einheitlich bereitzustellen. Dies würde durch eine breitere gesellschaftliche Akzeptanz und weniger Vorbehalte beim Einsatz in der Industrie (Wettbewerb) die Verfügbarkeit von Daten ausbauen und zugleich Systeme robuster machen.
- Gewährt man einer dritten Partei Einsicht in digitale Daten, erhält diese Partei zwangsläufig die Daten übermittelt – was faktisch mehr als nur eine Einsichtnahme ist. Daten müssten sich nach einer Einsicht selbst zerstören, z. B. über einen Einmalschlüssel.
- Es gilt die Akzeptanz technischer Systeme zu fördern. In der Gesellschaft besteht eine Ambivalenz zwischen selbstverständlicher Nutzung von z. B. Smartphones und einer eher verhaltenen Bereitschaft, sich mit den technischen Elementen auseinander zu setzen.
 - Auf Anwenderseite muss die Vertrauenswürdigkeit durch Transparenz gefördert werden. Es muss nachvollziehbar sei, was ein technisches System tut.
 - Auf Seiten der Ausbildung muss vermittelt werden, dass wir nur durch aktives Gestalten technischer Systeme unsere Gestaltungsfreiräume erhalten können (Wirtschaft / Gesellschaft).
- Wir brauchen Verfahren, um die Vertrauenswürdigkeit von Infrastrukturen zu prüfen und zu überwachen (Geräte, Hardware, Software, Services). Hierfür wird angeregt, gezielt entsprechende Forschungsprogramme aufzusetzen, z. B. zur Entwicklung von Methoden und (Software-) Lösungen zur Validierung der Vertrauenswürdigkeit von Systemen.
- Technische Systeme müssen zuverlässig funktionieren und einfach und nachvollziehbar bedienbar sein.
 - Dies erfordert u. a. eine stärkere Sensibilisierung, dass Technik für alle nutzbar sein muss,
 - eine Stärkung der Normung zur Gewährleistung der Interoperabilität und
 - intuitiv nutzbare Schnittstellen zu technischen Systemen.
- Wir brauchen insbesondere bei langlebigen Infrastrukturen die Fähigkeit, ihre Wartbarkeit langfristig durch Zugang zu Wissen und Ersatzteilen zu gewährleisten. Dies betrifft gerade auch die Software, wo ggf. der Quellcode kritischer Geräte in einer Art „escrow-Speicher“ hinterlegt wird.

- Bei Investitionen in die Schulbildung sollten nicht nur Anwendungen (digitales Klassenzimmer), sondern in Grundzügen auch die technischen Grundlagen der IKT, einschließlich der Software-Entwicklung / Programmierung vermittelt werden. Es gibt punktuell sehr gute Beispiele an Schulen, wo es gelingt, spielerisch aus der Anwendung das Interesse für Technik, und darüber für Physik zu wecken. Sehr preiswerte technischen Voraussetzungen sind heute gegeben (z. B. Raspberry Pi), es fehlt eher an entsprechend ausgebildeten Lehrkräften und der Möglichkeit, interessierte externe Experten (z. B. engagierte Ingenieure) für derartige Ausbildungen zu nutzen. Auch Patenschaften mit Universitäten oder Unternehmen können hier fördernd wirken.

5.3 Technologische Souveränität im breiteren (politischen) Kontext

Technologische Souveränität ist eingebettet in einen breiteren Kontext, der auch Resilienz und Nachhaltigkeit umfasst. In einzelnen Bereichen haben Technologien eine für den Wirtschaftsstandort Deutschland und den gesellschaftlichen Zusammenhalt essentielle Bedeutung erlangt. Dazu zählt die IKT.

- Gerade die Querschnittsbedeutung der IKT zeigt, dass wir heute dringender denn je technologiefeld- und branchenübergreifend in Systemen denken müssen. Dieses Selbstverständnis sollte aus den Branchen heraus eigenständig entwickelt werden. Die Erfahrung zeigt jedoch, dass es sehr schwer ist, aus einer bestimmten Branche kommend Verständnis für die Spezifika einer anderen Branche zu entwickeln. Hier kann die Politik als Moderator helfen, die unterschiedlichen Branchen zusammen zu bringen. Auch die interdisziplinäre Diskussion spezifischer Fragestellungen, wie z. B. im Münchner Kreis, hilft branchen-übergreifendes Verständnis zu entwickeln.
- Dieses Papier stellt im Schwerpunkt eine Methodik vor, ergänzt zur Erläuterung durch exemplarische, indikative Bewertungen. In ausgewählten branchenübergreifenden Initiativen sollten in einem ersten Schritt fundierte empirisch ermittelte Analysen für die wichtigsten Technologiefelder bzw. Schlüsseltechnologien erstellt werden. Im Zuge dessen könnte mit Hilfe der hier vorgestellten Methodik auch z. B. per Delphi-Verfahren ein Vergleich von Soll- und Ist-Werten der Bewertung technologischer Souveränität erfolgen. Daraus könnten dann präzise die drängendsten Aspekte identifiziert und Maßnahmen vorgeschlagen werden.
- Zur technologischen Souveränität gehört, dass Infrastrukturen robust aufgebaut und betrieben werden können und auch im Fehlerfall einzelner Bestandteile weiterhin zuverlässig funktionieren. Die Sicherstellung der Resilienz ist eine übergeordnete Anforderung, deren Gewährleistung auf politischer Ebene zu koordinieren ist, da hieraus für verschiedene Branchen, Technologiefelder und Wertschöpfungsstufen Souveränitätsanforderungen entstehen.

- Hierbei muss unbedingt auch die Software-Entwicklung im Blick behalten werden. Ohne die Fähigkeit, eigene Software mit modernen Entwicklungswerkzeugen und Architekturen zu entwickeln und zu betreiben, ist keine Infrastruktur betreibbar und nutzbar, funktioniert keine Logistik und keine Produktion.
- Eine weitere Grundvoraussetzung zu souveränem Handeln ist der Zugang zu Ressourcen. Bereits im Zuge von Handelskonflikten, wie wir sie derzeit vermehrt erleben, erhobene Zölle können den Zugang nicht nur zu Rohstoffen, sondern auch zu essenziellen Komponenten von Geräten empfindlich erschweren. Gerade die IKT ist hier besonders empfindlich, da viele Komponenten international bezogen werden müssen. Zugleich ist die IKT für sehr viele Branchen relevant und stellt für das gesamte öffentliche Leben eine kritische Infrastruktur dar. Dies betrifft nicht nur Rohstoffe oder bestimmte Komponenten und Produkte, wie z. B. Router, Speicher, Computer, Chips, sondern auch den Zugang zu Softwaretools, Algorithmen und Daten. Daher wird angeregt, auf politischer Ebene die Anforderungen an souveränes Handeln zu aggregieren und den Zugang zu den erforderlichen Ressourcen politisch zu gewährleisten (Verfügbarmachen auf nationaler / EU-weiter Ebene oder Liefermöglichkeiten aus verschiedenen Weltregionen).
- Ein weiterer Aspekt ist die Gewährleistung der Energieversorgung. International verkoppelte Energiesysteme sind anfällig, sodass sich Störungen in Netzen grenzüberschreitend auswirken. Gerade dezentrale Energiesysteme, wie sie für die regenerativen Energiequellen typisch sind, erfordern für ihr Management eine zuverlässige IKT. Andererseits ist eine stabile, zuverlässige und ausreichende Energieversorgung Voraussetzung für das Funktionieren der IKT. Ein spezifischer Aspekt ist hier der Zugang zu Rohstoffen für die Batterieherstellung.

6. Schlussfolgerungen

Deutschland und Europa müssen erkennen und akzeptieren, dass das geopolitische Umfeld, in das unsere Gesellschaft und Wirtschaft eingebettet sind, zunehmend von einer Rückbesinnung auf nationale bzw. Unionsinteressen geprägt wird. Hierbei werden technologische Abhängigkeiten zum Instrument der Politik, in einigen Fällen wird technologische Vorherrschaft sogar zum Politik- und Staatsziel erklärt. Definiert man technologische Souveränität als die Fähigkeit eines Staatswesens, seine politischen und gesellschaftlichen Ziele umsetzen zu können, ohne dabei von der Nichtverfügbarkeit oder dem fehlenden Zugriff auf spezielle Technologien behindert zu werden, dann ergibt das unmittelbar die Forderung, sich systematisch mit dem Thema der technologischen Souveränität auseinander zu setzen. In diesem Sinne äußerte sich auch bereits die Bundeskanzlerin und nannte in ihrer Rede im Deutschen Bundestag am 11. September 2019 u. a. die Bereiche Daten, Mikroelektronik und Batteriezellenfertigung als Beispiele für relevante Technologiefelder.

Dieses Positionspapier untersucht das Konzept und die zugrundeliegenden Abhängigkeiten der technologischen Souveränität im Detail. Es möchte hierbei unter anderem eine intensivere Diskussion anstoßen, wie wir uns in Deutschland bezüglich der Befähigung, Technologien souverän zu entwickeln und zu nutzen, aufstellen wollen.

Dazu schlägt es eine Systematik zur Identifikation von Technologiefeldern sowie Kriterien zur Bewertung der Technologiefelder vor. Der Begriff „Souveränität“ wird definiert und es wird eine Systematik vorgeschlagen zur Konkretisierung dessen, was Souveränität für einzelne Akteure entlang der Wertschöpfungskette bedeutet. Anhand von zwei Beispielen, 5G und KI in der Automatisierung, wird der Ansatz veranschaulicht.

Das Papier will einen Prozess anstoßen, mit dem mit definierten Kriterien sowohl relevante Technologiefelder als auch die aktuell dahinterstehenden Schlüsseltechnologien identifiziert werden. Mögliche Kriterien wurden in diesem Papier formuliert. In den Prozess sollen, soweit wie möglich, die verschiedenen Marktakteure aus den unterschiedlichen Branchen eingebunden werden. Sein Ziel ist aufzuzeigen, wo auf nationaler bzw. europäischer Ebene besondere Anstrengungen zur Erhaltung bzw. (Wieder-)Erlangung technologischer Souveränität erforderlich sind, wobei die konkreten Anforderungen an „technologischer Souveränität“ und ihr jeweils anzustrebender Grad im Rahmen des Prozesses ermittelt werden. Die Erfordernis eines branchenübergreifenden und damit politisch geführten Prozesses zeigt sich darin, dass in der IKT sehr viele verschiedene Technologien genutzt werden und damit Souveränitätsanforderungen an diese entstehen, und dass die IKT unverzichtbarer Bestandteil technischer Systeme in anderen Branchen geworden ist.

Auch wenn die Systematik unter dem Blickwinkel der Elektrotechnik / ITK entwickelt wurde, so möchte das Papier einen Beitrag zu einer einheitlicheren, branchenübergreifenden Systematik leisten, die es Entscheidungsträgern in Politik und Wirtschaft ermöglicht, relevante Technologiefelder zu identifizieren, die für diese Felder notwendige Souveränität abzuleiten und wo erforderlich in sowohl politische als auch wirtschaftsorientierte Maßnahmen umzusetzen.

Literaturverzeichnis

- Bau15 . . . Baums, A. Technologische Souveränität: Strategie oder PR-Hype. Oktober 2015. von www.digitale-standortpolitik.de abgerufen.
- Bit15 Digitale Souveränität: Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa. Berlin. BITKOM e.V. 2015
- Bit19 Digitale Souveränität: Anforderungen an Technologien- und Kompetenzfelder mit Schlüsselfunktionen. Berlin. BITKOM e.V. Dezember 2019
- Cle18 . . . Cleven, T. Huawei und 5G-Ausbau: „Deutschland muss seine digitale Souveränität zurückgewinnen“. Hannoversche Allgemeine. 11.12.2018. Von <http://www.haz.de/Nachrichten/Wirtschaft/Deutschland-Welt/Huawei-und-5G-Ausbau-SPD-Politiker-fordert-Deutschland-muss-seine-digitale-Souveraenitaet-zurueckgewinnen> abgerufen.
- CP00 . . . Technologische Vielfalt im Überblick. Vom Clusterportal Baden-Württemberg: <https://www.clusterportal-bw.de/clusterdaten/technologiefelder> abgerufen.
- Dew17 . . von Dewitz, W. (Juni 2017). Warum Bosch so viel wie nie in eine Fabrik investiert. manager magazin. Juni 2017. Von <https://www.manager-magazin.de/digitales/it/bosch-baut-chipfabrik-milliarden-investition-in-dresden-a-1152881-3.html> abgerufen.
- Eng00 . . . Engelhard, J. Branche. Von Gabler Wirtschaftslexikon: <https://wirtschaftslexikon.gabler.de/definition/branche-27701> abgerufen.
- GK16 . . . Gausemeier, J., & Klocke, F. Industrie 4.0 – Internationaler Benchmark, Zukunftsoptionen und Handlungsempfehlungen für die Produktionsforschung. Heinz Nixdorf Institut, Universität Paderborn, Werkzeugmaschinenlabor der Rheinisch-Westfälischen Technischen Hochschule Aachen. 2016.
- Han19 . . . Hua, S. China will ausländische Computer und Software aus seinen Behörden verbannen. Handelsblatt. 9.12.2019.
- Keu18 . . . Keupen, R. Die Bank als Plattform braucht ein Mindestmaß an technologischer Souveränität und Unterstützung. IT-Finanzmagazin. Oktober 2018.
- MR15 . . . Machnig, M., & Rohleder, B. Leitplanken Digitaler Souveränität. Nationaler IT-Gipfel. (BMW, Hrsg.) Berlin. 2015.
- Mai15 . . . Mair, S. Sicherheit durch technologische Souveränität. (BDI, Hrsg.). 2015.
- MRB18 . . Müller-Quade, J., Reussner, R., & Beyerer, J. Karlsruher Thesen zur Digitalen Souveränität Europas. Datenschutz und Datensicherheit, 42(5), 277–280. Springer Fachmedien. Mai 2018.
- NCA18 . . Nationales Cyber-Abwehrzentrum. Gefährungslage der Stromversorgung in Deutschland durch Cyberangriffe. 2018.
- OEC07 . . OECD (Hrsg.). Revised Science and Technology Classification in the Frascati Manual. Februar 2007. Von <http://www.oecd.org/science/inno/38235147.pdf> abgerufen.
- Wet16 . . . Wetzels, D. So fatal wäre ein Cyberangriff auf die globale Stromversorgung. Die Welt. 29. 09 2016. Von Wirtschaft: <https://www.welt.de/wirtschaft/article158440599/So-fatal-waere-ein-Cyberangriff-auf-die-globale-Stromversorgung.html> abgerufen.
- Wik19a . . Schlüsseltechnologie. November 2019. Von Wikipedia: <https://de.wikipedia.org/wiki/Schlüsseltechnologie> abgerufen.
- Wik19b . . Technological Readiness Level. Mai 2019. Von Wikipedia: https://en.wikipedia.org/wiki/Technology_readiness_level abgerufen.
- Wik20 . . . Digitale Souveränität. Januar 2020. Von Wikpidia: https://de.wikipedia.org/wiki/Digitale_Souveränität abgerufen.
- Zim07 . . . Zimmermann, K. (2007). Technologieklassifikationen und -indikatoren. Techn. Univ. Chemnitz. 2007. Von <https://nbn-resolving.org/urn:nbn:de:swb:ch1-200701448> abgerufen.
- ZVEI15 . . Diskussionspapier – Digitale Souveränität. ZVEI (Hrsg.). Juni 2015
-

Anhang

A. Fachgesellschaften

a. VDE

- Informations-Technische Gesellschaft (ITG)
- Energie-Technische Gesellschaft (ETG)
- Deutsche Gesellschaft für Biomedizinische Technik (DGBMT)
- GMM → VDI/VDE-Gesellschaft für Mikroelektronik, Mikrosystem- und Feinwerktechnik
- GMA → VDI/VDE-Gesellschaft für Mess- und Automatisierungstechnik

b. GI

- Betriebssysteme, Kommunikationssysteme und Verteilte Systeme (SYS)
- Datenbanken und Informationssysteme (DBIS)
- Graphische Datenverarbeitung (GDV)
- Grundlagen der Informatik (GInf)
- Informatik in Recht und Öffentlicher Verwaltung (RVI)
- Informatik in den Lebenswissenschaften (ILW)
- Informatik und Ausbildung / Didaktik der Informatik (IAD)
- Informatik und Gesellschaft (IUG)
- Künstliche Intelligenz (KI)
- Mensch-Computer-Interaktion (MCI)
- Sicherheit – Schutz und Zuverlässigkeit (SICHERHEIT)
- Softwaretechnik (SWT)
- Technische Informatik (TI)
- Wirtschaftsinformatik (WI)

c. VDI

- Bauen und Gebäudetechnik
- Energie und Umwelt
- Fahrzeug- und Verkehrstechnik
- Materials Engineering
- Mess- und Automatisierungstechnik
- Mikroelektronik, Mikrosystem- und Feinwerktechnik
- Produkt- und Prozessgestaltung
- Produktion und Logistik
- Technologies of Life Science (z. B. Bionik)
- Verfahrenstechnik- und Chemieingenieurwesen

B. Brancheneinteilungen

a. BMWI

- Automobilbau
- Bahnindustrie
- Bauwirtschaft
- Bergbau und Rohstoffe
- Bildungswirtschaft
- Biotech-Industrie
- Chemie und Pharmazie
- Elektrotechnik und Elektronikindustrie
- Energieversorgung
- Feinkeramische Industrie
- Feinmechanik und Optik
- Freie Berufe
- Gesundheitswirtschaft
- Gummi und Kautschuk
- Handel
- Holz und Möbelindustrie
- Informationstechnik und Telekommunikation

- Kredit- und Versicherungsgewerbe
- Kultur- und Kreativwirtschaft
- Lebensmittelindustrie
- Lederindustrie
- Lederwarenindustrie
- Luft- und Raumfahrt
- Maritime Wirtschaft
- Maschinen und Anlagenbau
- Papier und Druck
- Pflegewirtschaft
- Post
- Schuhindustrie
- Sicherheits- und Verteidigungsindustrie
- Sportwirtschaft
- Stahl und Metall
- Textil und Bekleidung
- Wasserwirtschaft
- Zweiradindustrie

b. Statista

- Agrarwirtschaft
- Bau
- Chemie & Rohstoffe
- Dienstleistungen & Handwerk
- E-Commerce & Versandhandel
- Energie & Umwelt
- Finanzen, Versicherungen, Immobilien
- Freizeit
- Gesellschaft
- Handel
- Internet [Apps, Nutzung]
- Konsum & FMCG
- Länder
- Leben
- Medien & Marketing
- Metall & Elektronik
- Elektroindustrie
- Feinmechanik & Optik
- Kraftfahrzeugbau
- Luft- & Raumfahrt
- Maschinen- & Anlagenbau
- Metallindustrie
- Schienenfahrzeugbau
- Schiffbau
- Pharma & Gesundheit
- Technik & Telekommunikation
- Fernsehempfang
- Festnetz & Mobilfunk
- Hardware
- Haushaltsgeräte
- IT-Services
- Software
- Unterhaltungselektronik
- Tourismus & Gastronomie
- Verkehr & Logistik
- Verwaltung & Verteidigung
- Wirtschaft & Politik

VDE Verband der Elektrotechnik
Elektronik Informationstechnik e.V.
Stresemannallee 15
60596 Frankfurt

Tel. +49 69 6308-0
Fax +49 69 6308-9865
info@vde.com
www.vde.com

VDE